United Nations S/AC.44/2004/(02)/5

Security Council

Distr.: General
14 October 2004

Original: English

**Security Council Committee established pursuant to resolution 1540 (2004)**

## Letter dated 12 October 2004 from the Deputy Permanent Representative of the United States of America to the United Nations addressed to the Chairman of the Committee

Enclosed is the United States report to the Security Council Committee established pursuant to resolution 1540 (2004). This report is a comprehensive review of United States laws, policies, projects, and initiatives to prevent illicit trafficking in weapons of mass destruction, their delivery systems, and related materials, and in particular to prevent terrorist acquisition of such items. It incorporates input from numerous agencies and presents a solid body of information on United States efforts related to the implementation of resolution 1540 (2004). The United States looks forward to continued cooperation with the Committee.

(*Signed*) Anne W. **Patterson**
Ambassador

04-56149 (E) 231104

**Annex to the letter dated 12 October 2004 from the Deputy Permanent Representative of the United States of America to the United Nations addressed to the Chairman of the Committee**

**United States report to the Committee established pursuant to resolution 1540 (2004)**

**Efforts regarding Security Council resolution 1540 (2004)**

*1. **Decides that all States shall refrain from providing any form of support to non-State actors that attempt to develop, acquire, manufacture, possess, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery;***

- As reiterated by President Bush in his February 11, 2004 speech to National Defense University, U.S. policy aims to prevent any form of support to non-State actors that attempt the activities listed in operative paragraph 1 of the Resolution.

- U.S. policy is also expressed in the **U.S. National Security Strategy**, a crucial aspect of which is the fight against all forms of terrorism, including those that comprise the use of WMD. An integral element of the National Security Strategy, the **U.S. National Strategy to Combat Weapons of Mass Destruction (December 2002)**, is a comprehensive effort to counter, in all of its dimensions, the threat posed by weapons of mass destruction (WMD) whether in the possession of hostile states or terrorists. In accordance with these strategies, the United States continues to work to strengthen both international and domestic U.S. nonproliferation efforts and to dissuade or impede those who seek to engage in prohibited activities. To this end, the United States adheres to multiple international treaties and multilateral regimes and has undertaken political commitments that prohibit such support. The United States also cooperates actively with other countries to strengthen barriers against proliferation to state or non-state actors of concern.

- U.S. law makes it a crime to provide material support or resources within the United States to a person intending to use the support or resources, or to prepare for, the commission of a wide variety of terrorism-related crimes, including specifically those involving weapons of mass destruction. These laws are described under Paragraph 2 of this report.

- The United States also maintains a wide array of domestic controls over relevant trade, transport, and commercial production activities as well as over financial transactions and services with a view to preventing non-State actor attempts to develop, acquire, manufacture, possess, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery. See Paragraph 3 of this report for a detailed description of these controls.

*2. **Decides also that all States, in accordance with their national procedures, shall adopt and enforce appropriate effective laws which prohibit any non-state actor to manufacture, acquire, possess, develop, transport, transfer or use nuclear, chemical or biological weapons and their***

***means of delivery, in particular for terrorist purposes, as well as attempts to engage in any of the foregoing activities, participate in them as an accomplice, assist or finance them;***

- To combat the proliferation of nuclear, chemical, or biological weapons, as well as their means of delivery, the United States has enacted, and vigorously enforces, a variety of domestic criminal laws. In particular, the U.S. law enforcement community endeavors to prevent future proliferation-related threats or attacks through the investigation and prosecution of individuals or entities involved in the illicit possession or movement of weapons of mass destruction (WMD).

- As a general matter, except under certain very limited circumstances, individuals in the United States are prohibited by federal criminal law from acquiring, transferring, or possessing materials that could constitute biological, chemical, or nuclear weapons. In accordance with its obligations under several international agreements, the United States has enacted national implementing statutes, which prohibit the illegal possession or transfer of such weapons. In addition, conspiracies, attempts, or threats to use such weapons are also proscribed.

- Executive Order 12333 assigns to the Director of the Federal Bureau of Investigation (FBI), under the supervision of the Attorney General and pursuant to such regulations as the Attorney General may establish, responsibility for conducting and coordinating counterintelligence (CI) activities in the United States against intelligence and terrorist activities conducted for, or on behalf of foreign powers, organizations, or persons. The **National Strategy for Counterintelligence**, dated August 2002, sets forth national priorities and strategic objectives for CI activities. In this context, the primary goal of the FBI's national Strategy for CI is to prevent or neutralize the foreign acquisition of nuclear, chemical, biological or other means of delivery-related information, technology, or equipment, which, if acquired, would constitute an immediate danger to the United States.

- The FBI is reorganizing its CI programs into a centralized, nationally directed, prioritized effort. By centralizing, the FBI has improved its ability to become more proactive and predictive in protecting the nation's WMD-related information and critical national assets. In particular, the FBI has placed full-time Special Agents at certain national laboratories and nuclear weapons production facilities to pursue matters within the FBI's investigatory purview.

*Nuclear Weapons*

- In the United States, no person may transfer, receive, manufacture, produce, acquire, possess, import, or export any nuclear weapon or nuclear explosive device except as provided by law. (42 U.S.C. § 2122). A violation of this provision subjects a person to ten years imprisonment or, alternatively, a life sentence, if he/she intended to injure the United States or secure an advantage to a foreign nation. (42 U.S.C. § 2272). Likewise, under U.S. law, a person may not receive, possess, use, transfer, alter, dispose of, or disperse any nuclear material, or nuclear byproduct material, which causes (or is likely to cause) death, serious bodily injury, or substantial damage to property or the environment. (18 U.S.C. § 831(a)).

- A person may also be subject to criminal liability for obtaining nuclear material through intimidation, fraud, or in an otherwise unauthorized manner. In addition, threatening to use nuclear material to injure persons or destroy property is prohibited. (18 U.S.C. § 831(a)). In this context, "nuclear material" means material containing any of the following: plutonium, uranium not in the form of ore or ore residue that contains the mixture of isotopes as occurring in nature, enriched uranium or uranium 233. These enforcement provisions are in accord with the treaty obligations under the Convention on the Physical Protection of Nuclear Material (ratified by the United States in 1982 with entry into force of the Convention in 1987).

  - The United States is actively working with its international partners to amend the CPPNM to include criminal prohibitions against nuclear smuggling and nuclear sabotage.

- Under U.S. law, the means of delivery for a nuclear weapon, such as rockets and missiles, likely will be deemed "destructive devices" and thus entail numerous criminal prohibitions. (18 U.S.C. § 921 et seq. and 26 U.S.C. § 5841 et seq.) Certain individuals (e.g. felons, illegal aliens) are categorically forbidden from possessing such devices, while the failure to register the devices with the federal government will subject a person to criminal prosecution. Domestic U.S. law also bars persons from teaching or demonstrating the use, or making, of a "destructive device or a weapon of mass destruction." (18 U.S.C. § 8424(p)(2)). Finally, accomplices who provide the "means of delivery" that enable others to illegally possess or use nuclear material are criminally liable as if they possessed or used the material themselves. (18 U.S.C. §§ 2, 831).[1]

- Depending on the circumstances, a person convicted of such an offense could face up to life imprisonment. (18 U.S.C. § 831(b), 18 U.S.C. § 844, 18 U.S.C. § 924).

*Chemical Weapons*

- Under U.S. law, a person may not develop, produce, otherwise acquire, transfer directly or indirectly, receive, stockpile, retain, own, possess, or use a chemical weapon. 18 U.S.C. § 229(a). Depending on the circumstances, a person convicted of such an offense faces up to life imprisonment. 18 U.S.C. § 229A(a)(1). If death results from the offense, the offender may also be subject to the death penalty. 18 U.S.C. § 229A(a)(2).

- These prohibitions and enforcement provisions are in accord with the treaty obligations under the Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction (1993).

  - Illustrative Cases:

    - In November 2003, a Texas man with ties to domestic anti-government groups pleaded guilty to possessing a sodium cyanide bomb. When he was arrested, the man also possessed a cache of pipe bombs and machine guns. He is currently serving an eleven-year term of imprisonment.

- In July 2003, a computer programmer who weaponized ricin was convicted in Spokane, Washington, for making a chemical weapon. Under U.S. law, ricin qualifies as both a biological and a chemical agent.

*Biological Weapons*

- Under U.S. law, a person may not develop, produce, stockpile, transfer, acquire, retain, or possess any biological agent, toxin, or delivery system for use as a weapon, or knowingly assist a foreign state or organization to do so. Depending on the circumstances, a person convicted of such an offense faces up to life imprisonment. 18 U.S.C. § 175(a).

- U.S. law also criminalizes the possession of biological agents, toxins, or delivery systems of a type or quantity that, under the circumstances, is not reasonably justified by a prophylactic, protective, bona fide research, or other peaceful purpose. 18 U.S.C. § 175(b). There is a ten-year statutory maximum for a violation of this provision.

- The impact of release of a highly dangerous biological agent or toxin – whether intentional or accidental – can be catastrophic. Thus, tight controls over such agents and toxins are paramount to prevent their use as a weapon or inadvertent release. Consequently, the United States strictly regulates possession, use, and transfer of certain biological agents and toxins ("select agents") that have the potential to pose a severe threat to public health and safety. These select agents and toxins are the "worst of the worst" and include biological agents such as bacillus anthrasis, yersinia perstis, clostridium botulinum, Plum pox potyvirus, Avian influenza virus (highly pathogenic), and the Bovine spongiform encephalopathy agent.

- On June 12, 2002, President George W. Bush signed into law the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 and the Agricultural Bioterrorism Protection Act of 2002. The Public Health Security and Bioterrorism Protection Act of 2002 authorized the strict regulation of the possession, use, and transfer biological agents and toxins (select agents and toxins) that have the potential to pose a severe threat to public health and safety. (42 C.F.R. Part 73) The Agricultural Bioterrorism Protection Act of 2002 authorized the strict regulation of select agents and toxins that have the potential to pose a severe threat to animal and plant health, or to animal and plant products. (7 C.F.R. Part 331, 9 C.F.R. Part 121) These select agents and toxins are "the worst of the worst" and include biological agents such as bacillus anthrasis, yersinia perstis, clostridium botulinum, Plum pox potyvirus, Avian influenza virus (highly pathogenic), and the Bovine spongiform encephalopathy agent.

- Under both Acts, individuals who have been identified as having a legitimate need to have access to select agents or toxins are required to undergo a security risk assessment conduct by the Department of Justice. Persons identified as "restricted persons" (e.g., convicted felons, persons indicted on felony charges, fugitives from justice, unlawful users of controlled substances, certain others), are prohibited from having access to select agents and toxins. (18 U.S.C. §175b) Additionally, a person who is reasonably suspected by an Federal law enforcement or intelligence

agency of committing an act of terrorism transcending national boundaries (as defined in 18 U.S.C. § 2332b(g)(5); knowing involvement with an organization that engages in domestic or international terrorism; or being an agent of a foreign power may also be denied access to select agents and toxins. A person violating the possession restrictions on select biological agents and toxins may be subjected to criminal prosecution. 18 U.S.C. § 175b.

- Among other improvements in the control of select agents and toxins are the regulatory requirements that those possessing, using, and transferring select agents and toxins must meet minimum established standards for biosafety, physical security, training, and record keeping.

- Another proactive feature of U.S. law involves the authority provided to the Attorney General to apply to a court for authorization to seize biological agents, toxins, or delivery systems if there is probable cause to believe that they would be used as a weapon. In an emergency, the Attorney General may act without a court order. 18 U.S.C. § 176.

- These prohibitions and enforcement provisions are in accord with the treaty obligations under the Convention on the Prohibition of the Development, Production, and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction (BWC) (1972).

- In August 2003, at the BWC Experts Group Meeting in Geneva, a prosecutor from the Counterterrorism Section of U.S. Department of Justice presented to the State Parties an overview of U.S. law enforcement efforts in the area of bioterrorism.

  - Illustrative Cases:

  - A computer programmer in Washington State who manufactured ricin as a biological weapon was convicted in July 2003. He later was sentenced to fourteen years in prison.

  - In late 2003, the United States prosecuted a medical researcher in Texas for inappropriately handling and transferring a select agent (Yersinia pestis). A jury convicted the researcher of, among other charges, shipping plague samples without the proper permit and mislabeling the mailing package. A federal court sentenced the researcher to two years imprisonment.

Finally, the Federal Bureau of Investigation continues vigorously to investigate the anthrax attacks in the Fall of 2001, which occurred in Florida, New York, and Washington, D.C. and killed five persons.

*Catch-all or General Provisions*

- Weapons of Mass Destruction – Apart from the foregoing specific provisions, U.S. law also prohibits anyone from using, or threatening, attempting, or conspiring to use, a "weapon of mass destruction." 18 U.S.C. § 2332a.

- A "weapon of mass destruction" is defined to include bombs, explosives, and any weapon that is designed or intended to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals, or their precursors, any weapon involving a biological agent, toxin, or vector or any weapon that is designed to release radiation or radioactivity at a level dangerous to human life. 18 U.S.C. § 2332a(c)(2).

- Depending on the circumstances, a person convicted of such an offense faces up to life imprisonment. If death results from the offense, the offender may also be subject to the death penalty. (18 U.S.C. § 2332a(a)).

- Hoaxes – In the aftermath of the anthrax attacks in Fall 2001, the United States experienced numerous false reports, or hoaxes, involving white powder substances purporting to contain anthrax. These hoaxes can seriously disrupt normal governmental or business operations while causing a needless waste of scarce emergency resources. Accordingly, the United States vigorously prosecutes hoax cases involving weapons of mass destruction.

  - A variety of criminal statutes provide the basis for such prosecutions. *E.g.*, 18 U.S.C. § 35(b) (prohibiting hoaxes concerning explosive or destructive devices when they impact motor vehicles, railroads, or shipping); 18 U.S.C. § 844(e) (hoaxes concerning bomb threats to buildings); 18 U.S.C. § 876 (mailing threatening communications); 18 U.S.C. § 1001 (providing material false statements); 49 U.S.C. § 46507 (hoaxes related to aircraft piracy).

- Demonstrating Use of WMDs – U.S. law prohibits not only the use of weapons of mass destruction but also bars teaching or demonstrating how to make or use a weapon of mass destruction to further a Federal crime of violence. 18 U.S.C. § 842(p)(2)(A). A person convicted of such an offense faces up to 20 years imprisonment.

- Material Support or Resources – Since the mid-1990's, U.S. law has prohibited the provision of "material support or resources" to terrorists or terrorist organizations. Instances involving the proliferation of biological, chemical, or nuclear weapons could potentially be prosecuted under these laws. 18 U.S.C §§ 2339A, 2339B.

  - "Material support or resources" is defined broadly to include "training," "expert advice or assistance," and "other physical assets," as well as financial support.

  - Providing material support is punishable by up to fifteen years imprisonment and, if death results, by a term of years or life imprisonment.

- Financial Transactions – Crimes involving the proliferation of biological, chemical, or nuclear weapons may also implicate the money laundering and forfeiture laws.

  - Pursuant to 18 U.S.C. §§1956 and 1957, whoever conducts or attempts to conduct a financial transaction knowing it to involve the proceeds of specified unlawful activity (SUA), or

engages in monetary transactions in property derived from specified unlawful activity, commits a money laundering offense. All property involved in "transactions or attempted transactions in violation of the money laundering statutes is subject to civil and criminal forfeiture." 18 U.S.C. §§ 981(a)(1)(A) and 982(a)(1). The quoted phrase encompasses not only laundering commissions, but also the property laundered, or any property derived from or traceable to such property, and any property that facilitated the laundering.

- Violation of the biological, chemical and nuclear nonproliferation statutes (18 U.S.C. §§ 175, 229, and 831) became money laundering SUAs in September 2001 when the USA PATRIOT Act added these crimes to the list of predicate crimes ("racketeering activity") under the Racketeer Influenced and Corrupt Organizations Act (RICO) 18 U.S.C. § 1961(1)(G). All RICO predicates are SUAs. 18 U.S.C. § 1956(c)(7)(A).

- The incorporation of the biological, chemical, and nuclear nonproliferation statutes into the RICO and the money laundering SUA list also made the proceeds of those violations forfeitable civilly under § 981(a)(1)(C) and forfeitable criminally under the combination of Section 981(a)(1)(C) and 28 U.S.C. § 2461(c), which was enacted as part of the Civil Asset Forfeiture Reform Act of 2000 (CAFRA) to make it possible to forfeit the proceeds of all SUAs both civilly and criminally. *Civil forfeiture proceedings are independent of a criminal prosecution and provide the basis for forfeiture irrespective of the status of the property owner, including when s/he is a fugitive, dead, or otherwise unavailable for prosecution.*

- In addition to making the proceeds of terrorism offenses forfeitable as just outlined, the USA PATRIOT Act also enacted a very broad terrorism forfeiture provision, 18 U.S.C. § 981(a)(1)(G), which makes forfeitable "all assets, foreign or domestic…of any individual, entity, or organization engaged in planning or perpetrating any act of domestic or international terrorism, as defined in18 U.S.C. § 2331, against the United States" or its residents and their property as well as all property acquired or maintained in connection with terrorism crimes, and property derived from, involved in, or used to commit such crimes. Section 981(a)(1)(G) is a civil forfeiture statute, and may be charged criminally in combination with 28 U.S.C. § 2461(c).

- In prosecuting crimes involving the proliferation of nuclear, chemical, and biological weapons, the United States may apply other statutes of general applicability that may fit the circumstances of a given case, including statutes pertaining to false statements, fraud, immigration violations, transportation of stolen property, etc.

- Prosecutorial resources dedicated to WMD proliferation prevention and prosecution include attorneys in the Counterterrorism Section of the Department of Justice's Criminal Division. These attorneys provide advice and guidance to federal prosecutors in U.S. Attorney's Offices around the country concerning investigative strategy, charging decisions and evidentiary questions in such cases. When necessary, attorneys from the Counterterrorism Section are available to assist U.S. Attorney's Offices in the trial of these cases. General oversight of these matters is provided

within the context of the Anti-Terrorism Advisory Council Program, with Regional Anti-Terrorism Coordinators within the Counterterrorism Section coordinating with and providing support to the Anti-Terrorism Advisory Council Coordinator in each U.S. Attorney's Office.

- Moreover, the Asset Forfeiture and Money Laundering Section in the Criminal Division has prosecutors who can provide advice and litigation assistance in pursuing actions to forfeit property involved in WMD related offenses and prosecuting related laundering offenses. Additionally, all United States Attorney's Offices have forfeiture units or attorneys dedicated to bringing forfeiture proceedings related to violations of federal statutes.

*Joint Terrorism Task Forces (JTTF)*

- The FBI has spearheaded the effort to share terrorism-related information among federal and state agencies by creating Joint Terrorism Task Forces (JTTFs). These are teams of state and local law enforcement officers, FBI agents, and other federal agents and personnel who work together to investigate and prevent acts of terrorism. Currently 66 JTTFs serve as important "force multipliers" in the war on terror, pooling multi-agency expertise and ensuring the timely collection and sharing of intelligence so critical to prevention efforts. More than 2,300 personnel work on these task forces nationwide.

- The National Joint Terrorism Task Force is located at the FBI command center in Washington DC. Nearly thirty agencies participate, spanning the fields of intelligence, public safety, federal, state, and local law enforcement. The National JTTF collects terrorism information and funnels it to the 66 JTTFs, to various terrorism units within the FBI, and to partner agencies. Agency representatives also help the FBI with terrorism investigations.

*Department of Homeland Security Information Sharing Initiative*

- DHS provides analysis of terrorist threats to the Homeland and compares the threats against vulnerabilities, through the Information Analysis and Infrastructure Protection Directorate, identified by the Department and its partners in this effort and shares information as widely as possible to detect, deter, and prevent acts of terrorism as well as to assist in dealing with the consequences of national and man made disasters such as acts of terror.

- The network used to share all available information with those who need it is called the Homeland Security Information Network. This network is patterned after the Markle Foundation "SHARE" network to provide multiple Communities of Interest (COI) and also to provide for information sharing and collaboration across any and all COIs through use of a common technology framework, whenever the need arises. Through the HSIN, the Department will soon provide connectivity to all of the States at a classified level to share classified intelligence on terrorists and their activities related to weapons of mass destruction.

***3. Decides also that all States shall take and enforce effective measures to establish domestic controls to prevent the proliferation of nuclear, chemical, or biological weapons and their means of delivery, including by establishing appropriate controls over related materials and to this end shall:***

***3(a) Develop and maintain appropriate effective measures to account for and secure such items in production, use, storage or transport;***

*Accounting for, and Securing, Nuclear Weapons*

- Department of Defense (DoD) Directives provide appropriate effective measures to account for and secure nuclear weapons and their means of delivery, storage or transport. Under Department of Defense Directive (DoDD) 3150 2, the DoD Nuclear Weapon System Safety Program provides general guidance in the form of four safety standards that govern all DoD nuclear stockpile operations. These four standards are:

  1. There shall be positive measures to prevent nuclear weapons involved in accidents or incidents, or jettisoned weapons, from producing a nuclear yield.
  2. There shall be positive measures to prevent DELIBERATE prearming, arming, launching, or releasing of nuclear weapons, except upon execution of emergency war orders or when directed by competent authority.
  3. There shall be positive measures to prevent INADVERTENT prearming, arming, launching, or releasing of nuclear weapons in all normal and credible abnormal environments.
  4. There shall be positive measures to ensure adequate security of nuclear weapons, under DoDD 5210.41.

- DoDD 5210.42, the Nuclear Weapon Personnel Reliability Program, provides guidance to ensure only properly screened and monitored personnel are permitted to conduct operations involving nuclear weapons. Only those personnel who have demonstrated the highest degree of individual reliability for allegiance, trustworthiness, conduct, behavior, and responsibility shall be allowed to perform duties associated with nuclear weapons, and they shall be evaluated continuously for adherence to PRP standards. The certifying official for military and DoD civilian personnel shall be the commander, or DoD military official, in a PRP position, responsible for nuclear weapons and/or NC2 operations having sufficient personal contact with all subordinate PRP personnel to permit continual evaluation of their performance and reliability. For DoD contractor personnel, the certifying official shall be the DoD military or civilian official designated in the contract.

*Transportation of Nuclear Weapons and Special Nuclear Materials*

- DOD Directive 4540.5 (Logistic Transportation of Nuclear Weapons) provides guidance for the safe and secure transportation of all nuclear weapons in DoD custody. Nuclear weapons require special consideration because of their political and military importance and the potential consequences of an accident, incident, or unauthorized act. The DoD Components shall take precautions to ensure that a nuclear weapon movement has minimal impact on public health, safety, and the environment. Nuclear weapon movements shall be kept to the minimum consistent

with military requirements and will be conducted through the transportation modes and movement routes that balance safety, security, and military requirements.

- The Department of Energy transports nuclear weapons, nuclear components, and other materials under guidelines authorized by Department regulations under the control of the Transportation Safeguards System (TSS). Only U.S. Government Federal Agents in the Department of Energy are authorized to have custody of nuclear weapons and components during the transportation between Government installations. All Federal Agents are qualified law enforcement officers, and in addition are specially trained and qualified in special response force tactics and armed defense. They participate in a security focused human reliability program designed to ensure that individuals with access to special nuclear materials, nuclear explosives, nuclear facilities and programs meet with highest standards of reliability as well as physical and mental suitability. The Department utilizes dedicated Government communications systems and specialized vehicles to ensure the safe and secure transport of all cargo.

- Additionally, specialized communications and specialized vehicles ensure the safe and secure transportation of DOE cargos containing nuclear weapons and special nuclear materials.

*Accounting for, and Securing, Nuclear Materials*

- Under the Atomic Energy Act of 1954, as amended (AEA),[2] and the Energy Reorganization Act of 1974, as amended (ERA),[3] the U.S. Nuclear Regulatory Commission (NRC) is the independent, non-Executive Branch Agency (separate from DOE) responsible for establishing and enforcing regulatory controls to ensure the safe and peaceful civilian use of byproduct, source and special nuclear materials.

- NRC regulatory controls, set forth in Title 10, Chapter 1, U.S. Code of Federal Regulations Parts 1-199 (10 CFR Parts 1-199), are designed to ensure adequate protection of public health and safety, promote the common defense and security of the United States, and protect the environment by establishing "defense-in-depth" or a series of mutually reinforcing licensing requirements.

- The National Nuclear Security Administration (NNSA), a separately organized agency within the Department of Energy, is responsible for maintaining and enhancing the safety, reliability, and performance of the United States nuclear weapons stockpile; directing, managing, and overseeing the nuclear weapons production facilities; and directing, managing and overseeing assets to respond to incidents involving nuclear weapons and materials under the authority in the Atomic Energy Act of 1954, Pub. L. No. 83-703, as amended, the Energy Reorganization Act of 1974, Pub. L. No. 93-438, as amended and the National Nuclear Security Administration Act, Pub. L. No. 106-65, 50 U.S.C. 2401, et seq., as amended.

- A series of Department of Energy directives contain requirements for accounting for and securing nuclear materials. These requirements are designed to ensure adequate protection of public health

and safety, promote the common defense and security of the United States and protect the environment by establishing a "defense-in-depth" safeguards and security program.

- The Department of Energy requirements apply to DOE-owned and DOE–leased facilities and DOE-owned nuclear materials at other facilities that are exempt from licensing by the NRC.

- NRC's licensing requirements apply to commercial nuclear power plants, research, test and training reactors, fuel cycle facilities, medical, academic and industrial users of nuclear materials as well as those who transport, store and dispose of nuclear materials and waste.

- To monitor and enforce licensees' compliance with regulatory requirements, NRC is authorized to:
  - Conduct inspections of licensee facilities and materials in their possession.[4]
  - Investigate suspected or reported instances of non-compliance.[5]
  - Issue "orders" to modify, suspend or revoke a license or require specific actions because of a public health issue.[6]

- The Department of Energy has multiple layers of oversight to monitor and enforce contractor's compliance with Departmental requirements. Department of Energy contractors are required to establish and implement a comprehensive internal review and assessment program for their materials control and accountability programs. Local federal oversight is afforded the contractor facilities by site or field offices. The Office of Independent Oversight and Performance Assurance evaluates the effectiveness of policies and Department-wide policy implementation in the areas of safeguards and security, cyber security, emergency management, and environment, safety and health.
  - Internal review and assessment programs provide for self-identification of areas of non-compliance and system deficiencies. The contractor is responsible for responding to the results of these reviews and developing and implementing appropriate corrective actions.
  - Federal oversight at both the local and Department-wide levels identifies findings, for which the facility contractor is responsible for developing and implementing appropriate corrective action plans. The findings and their associated corrective action plans and closure are tracked in a Departmental database.

- Willful violations of certain statutes and regulations governing the production, use, storage and transport of nuclear weapons and materials which may result in criminal prosecution and a range of criminal penalties.
- Both the DOE and NRC refer criminal investigations to the Department of Justice (DOJ) for possible prosecution.[7]

- Examples of criminal acts include:
  - Knowing and willful impairment of a basic component of a nuclear facility with the intent of adversely affecting operation and potentially harming public safety.[8]

- Unauthorized disclosure, tampering with, conspiring to communicate or conspiring to receive Restricted Data with intent to injure the United States or to secure an advantage to any foreign nation.[9]
- Interference with NRC or other federal inspectors to impede their efforts and prevent detection of regulatory violations or illegal activities.[10]
- Attempted or actual sabotage at a nuclear facility or to nuclear fuel licensed by NRC or under the purview of the Department of Energy.[11]

- NRC administers enforcement proceedings for civil (non-criminal) violations in accordance with regulations set forth in Subpart B of 10 CFR Part 2.[12]

- Both the U.S. Nuclear Regulatory Commission regulations (10 CFR Part 74) and Department of Energy directives require licensees or contractors possessing certain quantities or categories of special nuclear or source material[13] at fixed sites to establish and maintain material protection, control and accounting systems so as to promptly detect and prevent theft or unlawful diversion of the material.

- Required features of material control and accounting (MC&A) systems vary depending on the type of facility and material involved. Illustrative examples of required features include:
  - A distinct management structure, which assures clear overall responsibility for material control and accounting (MC&A) independent from production responsibilities;
  - Separation of key MC&A responsibilities via independent, objective management oversight to prevent insider collusion or some other adversarial act;
  - An effective personnel training and qualification program to ensure that personnel are technically capable of performing their responsibilities without degrading the effectiveness of the MC&A system;
  - Internal controls and procedures to track inventory and record information consistent with requirements specified for each category of material;
  - A recordkeeping system consistent with requirements specified for each category of material;
  - A measurement system to assure that all quantities in the material accounting records are based on measured values consistent with requirements specified for each category of material;
  - Process and item monitoring capabilities consistent with requirements specified for each category of material;
  - Procedures for controlling storage, handling and recording inventory data so that unauthorized removals of substantial quantities of material will be detected; and
  - Procedures for performing independent assessments of the effectiveness of the system and for maintaining records of improvements made as a result.

- NRC licensees are required to report incidents of theft, attempted theft or unlawful diversion of special nuclear material to the NRC Operations Center via the Emergency Notification System within one hour of discovery.

- Department of Energy contractors report incidents of theft, attempted theft or unlawful diversion of special nuclear material to the Department of Energy Emergency Operations Center within one hour of discovery.

- As part of the recordkeeping requirements, NRC licensees are required to provide source and special nuclear materials inventory data including details on domestic transfers as well as exports and imports of such materials to the Nuclear Materials Management and Safeguards System (NMMSS), which is the national nuclear materials control and accounting database jointly funded by DOE and NRC.

Accounting for, and Securing Chemical Weapons

- DOD Directive 5210.65 established the U.S. Army as the lead agency that accounts for chemical weapons munitions and manages a supporting database. The Army's CW Implementation and Compliance Plan provides the roadmap for Army implementation of the CWC. Strict accountability measures are implemented during the delivery and receipt of chemical weapons at U.S. destruction facilities and during the actual destruction of the weapons.

- The DoD continually assesses potential threats to ensure effective physical security measures are in place to protect the CW stockpile and their means of delivery from theft or diversion. Department of Defense Directive 5210.65 specifically addresses requirements for safeguarding chemical agents and chemical weapons awaiting destruction. Accordingly, AR 190-59 (Chemical Agent Security Program) contains U.S. Army policies and procedures to prevent sabotage, theft, loss, seizure, or unauthorized access or use of CW while in storage and during transport, regardless of location. This regulation also sets guidelines for emergency response to a security-related incident, including at a chemical agent "exclusion area" that is wrongfully penetrated. Finally, Army regulation AR 50-6 sets out policies and procedures that provide rigorous personnel reliability and safety measures for those with access to chemical agents, chemical weapons, and chemical weapon destruction site activities.

- Army Regulations 50-6 and 190-59 require special security measures for transporting chemicals not prohibited by the CWC as well as for recovered chemical munitions which must be brought to chemical weapons storage or destruction sites. The CWC only permits movement of chemical weapons from a storage site to a destruction destination. Since each chemical weapons storage area is co-located with a chemical weapons destruction facility in a highly secured area, transport of chemical weapons to a destruction facility is exceptionally secure.

*Accounting for, and Securing Biological Materials*

- The United States uses a "**Select Agents**" list as the basis for accounting measures, personnel controls, and other security procedures appropriate to ensure the secure handling and transfer of biological agents and toxins. Criteria for establishing lists of select agents are set forth under both the Public Health Security and Bioterrorism Response Act of 2002 and the Agricultural

Bioterrorism Protection Act of 2002. (the Bioterrorism Acts). These regulations provide a list of biological agents and toxins having the potential to pose a severe threat to human public health and safety (HHS Select Agents and toxins); animal or plant health or to animal and plant products (USDA Select Agents and toxins); or to both human and animal health (Overlap Select Agents and toxins). Some of these agents also have the potential to be used as weapons.

- The Select Agent regulations require that persons who want to possess, use, or transfer select agents and toxins must register with either the U.S. Department of Health and Human Services (HHS), U.S. Department of Agriculture, or both. Such persons must be trained in handling, storing, disposing of, and transferring select agents, establish record-keeping accounts, implement integrated safety and security plans to prevent unauthorized access, establish emergency response plans, submit to U.S. government inspections, and notify relevant authorities immediately in the event of theft, loss, or release.

- The Bioterrorism Acts also require the United States Attorney General to conduct a security risk assessment of any individual identified as having a need to access a select agent or toxin to determine whether that person is a "restricted person" as that term is defined by 18 U.S.C. §175b; or whether the individual is reasonably suspected by any Federal law enforcement or intelligence agency of violating any of the offenses listed in 18 U.S.C. § 2332B(g)(5); having knowing involvement with an organization that engages in domestic or international terrorism; or being an agent of a foreign power as defined in 50 U.S.C. § 1801.

- The Bioterrorism Acts directs the HHS Secretary or USDA Secretary to deny access to select agents and toxins to individuals whom the Attorney General has identified as "restricted persons;" and to limit or deny access to such agents and toxins by individuals whom the Attorney General has identified as falling under the remaining categories listed above.

- An entity registered to possess, use, or transfer select agents or toxins must develop and implement safety, security, and emergency response plans and demonstrate that such plans continue to meet the entity's needs. See Biocontainment, security, and incident response plans (7 CFR § 331 -- plant) and Biosafety, security, and incident response plans (9 CFR § 121 -- animal), and Safety, Security and Emergency Response plans (42 CFR § 73 -- human). Federal regulations require that these plans be reviewed annually and revised as necessary to ensure that they continue to meet an entity's biosafety, containment, and security needs. In addition, drills or exercises must be conducted at least annually to test and evaluate the effectiveness of the plans and the plans must be reviewed and revised, as necessary, after any drill or exercise and after any incident.

- Such entities must, among other items, include in their security plans the following security requirements (or implement measures to achieve an equivalent or greater level of security):

  1. Allow unescorted access only to approved individuals who are performing a specifically authorized function during hours required to perform that job;

2. Allow individuals not approved under the regulations to conduct routine cleaning, maintenance, repairs, and other non-laboratory functions only when escorted and continually monitored by approved individuals;

3. Provide for the control of access to containers where select agents and toxins are stored by requiring that such containers be locked when not in the direct view of an approved individual and by using other monitoring measures, as needed;

4. Establish a protocol for intra-entity transfers, including provisions for ensuring that the packaging and movement is conducted under the supervision of an approved individual;

5. Require that approved individuals do not share with any other person their unique means of accessing the area or select agents or toxins; and

6. Require that approved individuals immediately report any of the following to the responsible official: any loss or compromise of keys, passwords, combinations, etc.; any suspicious persons or activities; any loss or theft of select agents and toxins; any release of a listed agent or toxin; and any sign that inventory and use records for select agents and toxins have been altered or otherwise compromised.

*Accounting for Certain Toxic Chemicals and Precursors*

- Pursuant to the Chemical Weapons Convention (CWC) and the U.S. Chemical Weapons Convention Implementation Act of 1998, U.S. CWC Regulations (15 C.F.R. §§ 710-729) impose annual declaration requirements to account for the production, processing, consumption, export and import of certain toxic chemicals and precursors related to chemical weapons. These regulations also require U.S. chemical companies to retain records related to declared activities involving subject chemicals for up to five years and to undergo on-site verification by international inspection teams. The Department of Commerce is the lead agency for routine and challenge inspections conducted at declared U.S. facilities not owned or leased by the Departments of Defense or Energy. These inspections require companies to demonstrate that declared activities are consistent with the objectives of the CWC through, inter alia, material balance checks of inventory, production, and transfer logs, and visual inspection of equipment for appropriateness of use.

***3(b): Develop and maintain appropriate effective physical protection measures:***

*Physical Protection Measures for Nuclear Weapons*

- Department of Defense (DoD) Directives provide appropriate effective physical protection measures for nuclear weapons, nuclear materials and their means of delivery (i.e. delivery vehicles). The foundation Directive is DoDD 5210.41, Security Policy for Protecting Nuclear Weapons. This directive lays out the basic tenets for maintaining the security of U.S. nuclear forces and states that it is DoD policy to protect nuclear weapons from loss, theft, sabotage,

unauthorized use, and unauthorized or accidental damage or destruction. This directive also requires positive measures to ensure the complete physical control of nuclear weapons during all phases of their life cycle. To ensure a balanced security system, physical security procedures for forces (personnel, weapons, and all associated equipment necessary for nuclear operations) and facilities are combined.

- The Department of Energy policy for safeguards and security programs identifies and characterizes potential adversary threats to all laboratories, plants and facilities, personnel, property and information, specifically: nuclear weapons; nuclear weapon components, Special Nuclear Material (SNM) and nuclear material; chemical weapons awaiting demilitarization; chemical and biological agents retained in compliance with U.S. policy and treaty regulations; classified matter and proprietary information.

- It is the policy of DOE to protect against; unauthorized access; theft, diversion, sabotage; espionage/foreign intelligence collection; and loss of control of nuclear weapons, radiological, chemical or biological agents, weapons components, special nuclear material, classified matter and information, associated technologies, hardware and critical technologies at DOE facilities.

- It is the policy of DOE to protect against loss or theft of sensitive information or Government property and other acts which may cause unacceptable adverse impacts on national security, the health and safety of employees, the public, or the environment.

- The DOE baseline security policy is called the Design Basis Threat (DBT) and is used to.

  - Develop requirements for safeguards and security programs that provide a basis for planning, implementation and facility design;
  - Provide a basis for evaluation of implemented systems;
  - Support counterintelligence programs and requirements; and
  - Provide a basis for evaluation of foreign and domestic intelligence collection risks posed to DOE interests.

- A fundamental principle of the Department's safeguards and security program is a graded approach. This approach applies to and is embodied in the relevant threat considerations for departmental assets. The rationale employed in grading the threat considers and accounts for factors such as consequence of the event, the attractiveness of the asset, the ability of the adversary to accomplish a given objective with an asset, the ability of an adversary to accomplish a given objective based on the adversary's postulated capabilities or actions, and the resources required by an adversary to accomplish a given objective.

- The graded threat approach entails the establishment of "Threat Levels" for departmental facilities and associated "Protection Strategies" based on the assets located at a given facility. The theft, disruption of mission and espionage/foreign intelligence collection targeting levels establish the baseline categorization of Departmental assets and facilities relative to the threat to those assets.

**Threat Level 1:** Facilities that manufacture, store, transport, or test nuclear weapons, nuclear test devices, or completed nuclear assemblies.

**Threat Level 2:** Facilities that receive, use, process, transport, or store high risk specified quantities of special nuclear material (SNM).

**Threat Level 3:** Facilities that receive, use, process, transport, or store lower risk quantities of SNM, Strategic Petroleum Reserve facilities, and Power Marketing Administration facilities.

**Threat Level 4:** Facilities defined as having low risk quantities of SNM or quantities of other nuclear materials of significant monetary importance (valued at $5,000,000 or more) or which support the enduring nuclear weapons stockpile, or non-fissile weapon components. Facilities that house critical National security assets, missions or personnel. DOE National Nuclear Security Administration (NNSA) field and Headquarters (HQ) facilities.

**Threat Level 5:** All other facilities including those that are only required to maintain minimum safeguards accountability or security operations (e.g., isolated small DOE activity office, office tenant in a larger office building, small isolated research or test facilities).[14]

- Specific details of on-site security equipment, tactics and operations are determined by the local site manager and are to correspond to the facility mission.

*Physical Security of Nuclear Materials Used for Civilian Purposes*

- NRC regulations (10 CFR Part 73) require licensees to implement and maintain various levels of physical protection for nuclear material and facilities. Physical protection requirements are implemented in a graded approach commensurate with the consequences associated with the loss of special nuclear material or sabotage of nuclear facilities.

- The levels of physical protection required are designed to prevent incidents of radiological sabotage and theft or diversion of material.

- Key physical protection requirements for nuclear reactors, fuel cycle facilities, and spent fuel storage and disposal facilities include:

  - Multiple physical protection barriers and access controls consistent with the sensitivity of each of the areas protected (i.e., defense-in-depth).
  - Intrusion detection capabilities
  - Detection alarms to distinguish between false or nuisance alarms and actual intrusions
  - Response plans and procedures to deal with intrusions, and
  - Communication channels and protocols for obtaining off-site assistance, as necessary, from local, State, and Federal agencies.

- Key physical protection requirements for transporting spent nuclear fuel and other high activity shipments include:

  - Use of NRC-certified, structurally rugged, shipment overpacks and canisters.
  - Advance planning and coordination with local law enforcement along routes.
  - Protection of information about schedules.
  - Regular communication between transporters and control centers.
  - Armed or unarmed escorts, depending on the material.
  - Vehicle immobility measures to protect against movement of a hijacked shipment before response forces arrive.

- Physical protection also includes licensee security guard force personnel, who, for many facilities are armed and capable of using deadly force if necessary to defend against attacks.

*Physical Security of Nuclear Weapons Production Sites*

- The process for securing Department of Energy nuclear weapons production and materials sites is based on DOE's Site Safeguards and Security Plans (SSSP). These plans require documentation, and, as appropriate, upgrades to overall site protection.

- The Department of Energy gives specific consideration to the following best practices, set out below.

1. **Design Basis Threat**: Adversary numbers, characteristics, capabilities. National and local level threat assessments.

2. **Graded approach for material assets**; provide the most security to the material whose loss has the greatest consequence. National authority should determine material grades.

3. **Design** a security system to protect against the threat. Determine strategy; containment or denial.

4. **Documentation** of security posture in Site Safeguards and Security Plan.

5. **Vulnerability Assessments**. Computer based modeling; expert based judgements.

6. **Performance Testing**. Worse case scenarios – force on force exercises.

7. **Iterative Site Analysis**. "Testing to failure", realistic modeling and timelines.

8. **Independent Assessments**. Conducted by an oversight organization independent of operations.

9. **Human Reliability Program**. A security and safety reliability program designed to ensure that individuals who occupy positions affording access to certain materials, nuclear explosives, facilities and programs meet the highest standards of reliability and physical and mental suitability

10. **Creation of a "Security Culture"** – Integrated Safeguards and Security Management.

*Physical Protection Measures for Chemical Weapons*

- The U.S. Department of Defense Directive 5210.65 specifically addresses requirements for safeguarding chemical agents and chemical weapons, including their means of delivery. Accordingly, the U.S. Army implements chemical surety and security programs (AR 50-6) to ensure personnel reliability and safety in accessing chemical agents, chemical weapons and chemical weapon destruction site activities. Under AR 190-59, the Army enforces strict physical security controls for safeguarding the U.S. CW stockpile and their means of delivery, while they await destruction.

- The United States has enacted measures to implement fully its obligations under the OPCW inspection regime, which contributes to global efforts under the CWC to foreclose diversion of sensitive chemicals and to prevent chemical weapon proliferation.

*Physical Protection Measures for Biological Materials*

- The Select Agent Rule establishes specific physical security requirements for handling listed biological agents. HHS and Agriculture have established requirements, guidelines, and guidance covering laboratory safety (biosafety), laboratory security (biosecurity), transportation of infectious substances, outbreak and containment advisories, radiation and chemical safety, facility emergency response programs, employee occupational health programs, and the development of employee training and outreach initiatives in these areas. In addition, HHS works with WHO, the Pan American Health Organization, the World Organization for Animal Health (OIE), and the UN Committee of Experts on the Transport of Dangerous Goods, and others in developing international guidelines and guidance taking into account U.S. domestic requirements and experience.

***3 (c) Develop and maintain appropriate effective border controls and law enforcement efforts to detect, deter, prevent, and combat, including through international cooperation when necessary, the illicit trafficking and brokering in such items in accordance with their national legal authorities and legislation and consistent with international law;***

*Border Controls*

- The Department of Homeland Security and its agencies (principally Immigration and Customs Enforcement (ICE), Customs and Border Protection (CBP), the United States Coast Guard

(USCG), and the Transportation Security Administration (TSA)) exercise substantial domestic legal authorities in connection with border control to interdict and prevent the illegal introduction, export or transit of weapons of mass destruction (WMD), missiles, and related components, precursors and technologies in the United States. Where such items are being imported, exported, or are transiting U.S. land borders, waters or airspace, a variety of U.S. customs, export control, transportation security, and criminal laws provide authority for the performance of law enforcement and homeland security functions, including screening, search, detention, seizure, arrest, and investigation of persons, cargo, merchandise and conveyances.

- ICE and CBP officers may conduct inbound and outbound searches of merchandise, cargo, and conveyances and non-intrusive searches of persons at the border without a warrant. Additional law enforcement powers are conferred upon CBP and ICE officers pursuant to the Tariff Act of 1930, as amended, and the Immigration and Nationality Act, as amended. See, e.g., 19 U.S.C. 482, 1589a, 1499, 1581, 1582, 1595a, and 8 U.S.C. 1357. Beside the border enforcement authorities, ICE agents (and to some extent CBP agents) are also authorized to exercise traditional federal law enforcement powers that include the ability to make arrests, serve warrants, conduct undercover operations, carry firearms, conduct electronic surveillance, exchange information, summons records and testimony, and in conjunction with CBP, pursue civil and criminal sanctions, including the forfeiture of property, proceeds, and conveyances used in or derived from the illegal import or export of articles contrary to law. See 18 U.S.C. §§ 545, 19 U.S.C. 1595a, and 22 U.S.C. § 401.

- TSA has broad statutory authority for security in all modes of transportation, while DOT and its modal administrations exercise authority in this area primarily over transportation safety matters. Under authorities enumerated in the Aviation and Transportation Security Act (ATSA, Pub. L. 107-71, 115 Stat 597 (November 19, 2001) and delegated by the Secretary of Homeland Security to the Administrator of TSA, the Administrator's broad responsibility for security in all modes of transportation includes the security of mass transit. See 49 U.S.C. § 114(D). Further, in accordance with paragraph 15 of Homeland Security Presidential Directive – 7 (HSPD-7), which was issued December 17, 2003, the Secretary of Homeland Security has the lead role in coordinating protection activities for "transportation systems, including mass transit, aviation, maritime, ground/surface, and rail and pipeline systems."

- See 49 U.S.C. § 114(d) in executing those responsibilities and duties, the Administrator is empowered, among other things, to:

  (1) Assess threats to transportation, 49 U.S.C. § 114(f) (2);
  (2) Develop policies, strategies and plans for dealing with threats to transportation, 49 U.S.C. § 114(f) (3);
  (3) Make other plans related to transportation security, including coordinating countermeasures with appropriate departments, agencies, and instrumentalities of the United States Government, 49 U.S.C. § 114(F)(3);
  (4) Enforce security-related regulations and requirements, 49 U.S.C. § 114(F)(7);

(5) Oversee the implementation, and ensure the adequacy of security measures at airports and other transportation facilities, 49 U.S.C. §114(f)(11), and

(6) Issue, rescind, and revise such regulations, including issuing regulations and security directives (SDs) without notice or comment or prior approval of the Secretary, as are necessary to carry out TSA functions, 49 U.S.C. § 114(1) (l) and (2).

- The U.S. Coast Guard (USCG) is the lead maritime law enforcement agency responsible for maritime and port security. Qualified Coast Guard law enforcement personnel may "make inquiries, examinations, inspections, searches, seizures, and arrests upon the high seas and waters over which the United States has jurisdiction, for the prevention, detection, and suppression of violations of laws of the United States." See 14 U.S.C. 89. Coast Guard personnel may also carry firearms and make arrests at any structure or facility of any kind located in, on, under, or adjacent to any waters subject to the jurisdiction of the United States. See 46 U.S.C. § 70118; 33 U.S.C. § 1226 (b) (3).

- With respect to U.S.-flagged vessels on the high seas, the Coast Guard has plenary power to stop, board, and inspect those vessels without any suspicion of criminal activity. During such inspections, where probable cause develops, the Coast Guard may take further law enforcement authority consistent with U.S. domestic law. With respect to foreign-flagged vessels, the Coast Guard may take law enforcement action pursuant to agreements or arrangements between the United States and the flag country of the vessel in question, or as is otherwise consistent with international law.

- In addition to its general law enforcement authority, qualified Coast Guard law enforcement personnel are also customs officers and in coordination with ICE and CPB, these Coast Guard personnel may conduct border searches and exercise other customs authorities. See 14 U.S.C. §142, 19 U.S.C. § 1401, 19 U.S.C. §1589a. Within the U.S. territorial sea the Coast Guard exercises authority for the protection and security of vessels, harbors, and waterfront facilities. See Magnuson Act, 50 U.S.C. § 191, and 33 C.F.R. Part 6; Ports and Waterways.

*The International Emergency Economic Powers Act, 50 U.S.C. 1702 ("IEEPA") and the Trading with the Enemy Act, 50 U.S.C. App. 1, et seq. ("TWEA").*

- The President may declare embargoes or limit certain activities with respect to foreign countries. ICE and CBP officers enforce import/export embargoes and restrictions under IEEPA and TWEA, in coordination with the Treasury Department's Office of Foreign Assets Control.

*The Money Laundering Control Act of 1986, as amended, 18 U.S.C. 1956-1957, 1960, 981-982, 984, and 986, and the Bank Secrecy Act ("BSA"), 31 U.S.C 5311-22.*

- CBP and ICE officers are charged with enforcing the BSA reporting requirements for the transportation of monetary instruments under 31 U.S.C. 5316. Under section 5316, the transportation of currency or other monetary instruments exceeding $10,000 into or out of the

United States must be reported to a Customs officer. Under 31 U.S.C. § 5317, Customs officers have border search authority to examine persons, baggage, cargo, envelopes and conveyances without a warrant to ensure compliance with these reporting requirements. Currency and other monetary instruments that are not reported or that are falsely reported are subject to seizure and civil forfeiture. In addition, any property traceable to monetary instruments transported in violation of the reporting requirements is subject to civil forfeiture.

- ICE and CBP officers also enforce the Money Laundering Control Act, 18 U.S.C. § 1956-57 ("MLCA"). Specifically, ICE officers enforce money laundering violations involving smuggling and customs fraud offenses; export control offenses; violations of the BSA reporting requirements for international transportations; and import and export offenses involving stolen property, intellectual property rights, and obscene materials.

*Customs Laws*

- Customs laws include civil and criminal provisions relating to the importation process dating from the Tariff Act of 1930 and its antecedents, such as smuggling into the United States (18 U.S.C. § 545); into a foreign country if that country has similar provision (18 U.S.C. § 546); false statements; entry by means of a false invoice, declaration, etc. (18 U.S.C. § 542); entry with a false classification (18 U.S.C. § 541); customs civil fraud (19 U.S.C. § 1592); sanctions for importations contrary to law (19 U.S.C. § 1595a); and failure to declare (19 U.S.C. § 1497).

*Atomic Energy Act*

- The unauthorized export of nuclear material, nuclear weapons, and production facilities is prohibited. 42 U.S.C. §§ 2077, 2122, 2131. CBP inspectors ensure that all exports of nuclear material comply with the licenses and requirements of the Nuclear Regulatory Commission.

- NRC makes information on advance notifications for selected high risk radioactive sources available to CBP inspectors and serves as an information resource on questions regarding the legitimacy of certain radioactive materials exports or imports.

*Export Authority*

- ICE and CBP officers enjoy the same broad enforcement authorities for export compliance as they do for import compliance. This includes the authority to -

a. Conduct warrantless border searches of persons, cargo, baggage and conveyances destined for export.
b. Inspect all documents relevant to exports.
c. Question all individuals involved in exporting.
d. Prohibit lading of suspect shipments for export.
e. Detain and seize any shipments being exported in violation of law.
f. Prevent the departure of any carrier used to export illegally.
g. Order the unloading of carriers being used to export illegally.
h. Order the return of commodities exported illegally.

ICE officers also have warrantless arrest authority for federal export offenses (See 19 U.S.C. 1589a) and may make warrantless seizures of articles intended for illegal export, and conveyances facilitating such violations. See 22 U.S.C. 401.

*Container Security Initiative*

- Maritime security is a vital entity to both global security and trade. Ensuring the security of the maritime trade system is essential because approximately 90% of the world's cargo moves by sea container.

- CBP Commissioner Robert C. Bonner initiated the Container Security Initiative (CSI) on January 17, 2002 in an effort to address the threat to border security and global trade posed by the potential use of containerized shipping to conceal a WMD. The consequences of the use of containerized shipping by terrorists would be devastating, however, the implementation of greater security does not have to mean slowing down the flow of trade. CSI achieves a balance between security and the facilitation of legitimate trade.

- CSI is a four-part program designed to achieve a more secure maritime trade environment. CSI's four core elements include, establishing security criteria to identify high-risk containers; pre-screening those containers identified as high-risk prior to arrival to U.S. ports; utilizing technology to quickly pre-screen high-risk containers; and developing and using smart and secure containers.

- In the event a cargo container is targeted and rejected due to potential WMD concerns, it will not be permitted to continue on its course to a U.S. port. Moreover, if the container is loaded onto a ship bound for a U.S. port, that ship will not be allowed into U.S. territorial waters. If, on the other hand, a container is targeted for inspection for commercial reasons, and is not inspected in the foreign port, it will be inspected when it reaches a U.S. port.

- Initially, CSI's implementation objective focused on addressing the top 20 foreign seaports that represent the greatest volume of containerized cargo. Governments from these 20 foreign ports have already agreed to implement CSI. To date, CSI teams have been deployed to three fronts in the war on terrorism, the European front, the African front, and the Asian front. CSI is currently expanding its focus to include additional ports based on volume, location and strategic concerns provided that they meet all minimum standards set forth by the program. The continued expansion of CSI will include ports in areas such as South and Central America, Southeast Asia, and the Middle East.

- Under CSI, small groups of well-trained, experienced, CBP and ICE personnel are being deployed to work with host nation counterparts to target high-risk containers. When a potentially high-risk container is detected, these teams, working with their host counterparts, use non-intrusive inspection (NII) (gamma and x-ray devices) to ensure concerns regarding the container and its contents are addressed before it is loaded on a ship. The Trade Act, (P.L. 107-210, as amended by P.L. 107-295), which mandates that 100 percent of electronic manifest information be sent to CBP at least 24 hours before sea container cargo is loaded on board the vessel, allows the teams to target sea containers prior to their loading. In the event that a physical anomaly is detected, the host customs officers screen and examine the container while the CBP officers observe the process. By working with other nations and their customs administrations, CBP can jointly achieve far greater security for maritime shipping than by working independently.

- CSI offers participating countries the opportunity to send their customs officers to major U.S. seaports to target ocean-going, containerized cargo to be exported to their countries. CBP also shares information on a bilateral basis with its CSI partners.

*Radiation Detection Equipment and Non-Intrusive Inspection Imaging Technology*

- CBP has developed and implemented a comprehensive strategy to detect, deter, prevent and combat the trafficking and brokering of illicit nuclear and radiological materials. An integral part of CBP's comprehensive strategy to combat nuclear and radiological terrorism is to screen all arriving trucks, containers, trains, cars, airfreight, mailbags and express consignment packages with radiation detection equipment prior to release.

- CBP employs radiation detection equipment and large-scale non-intrusive inspection (NII) imaging technology at ports of entry to screen shipments for the presence of illicit radioactive and nuclear materials. These technologies include: radiation portal monitors (RPM), radiation isotope identifier devices (RIID), personal radiation detectors (PRD) and large-scale NII imaging systems. Large-scale NII imaging systems and RPMs enable CBP to quickly and effectively screen conveyances and cargo for illicit materials while the PRDs and RIIDs enable CBP officers to safely conduct examinations of those shipments suspected of containing illicit radiological materials. Used in combination, these tools provide CBP with a significant capacity to detect illicit nuclear or radiological materials and weapons while facilitating the flow of legitimate trade and travel.

- The CBP is also assisting the U.S. Nuclear Regulatory Commission on the creation of a centralized database to track all nuclear or radiological materials of concern.

- As of August 12, 2004, CBP has deployed 284 RPMs and 151 large-scale NII imaging systems to our ports of entry. Additionally, CBP has deployed over 10,000 PRDs and over 360 RIIDs to our ports of entry. Furthermore, as part of the comprehensive strategy noted above, CBP is in the process of developing and securing robust technology to detect, deter, prevent, and combat the illegal trafficking and brokering of illicit chemical and biological weapons or their precursors.

*Public Health Activities*

- The Bioterrorism Acts direct the HHS or USDA Secretaries to deny access to select agents and toxins to individuals whom the Attorney General has identified as "restricted persons;" and, limit or deny access to such agents and toxins by individuals whom the Attorney General has identified as falling under the remaining categories. The HHS Inspector General has authority to conduct investigations and to impose civil money penalties against any individual for violation of the Select Agent regulations.

    - Restricted persons include: aliens (other than those lawfully admitted for permanent residence) who are nationals of countries that the Secretary of State has determined have repeatedly provided support for international terrorism; persons under indictment for, or convicted of, a felony; fugitives from justice; unlawful users of controlled substances; illegal aliens; person adjudicated as mentally defective or committed to a mental institution; and persons dishonorably discharged from the Armed Services of the United States.

- Additional resources have been allocated for the expansion and enhancement of CDC Quarantine Stations at major international airports. Currently CDC operates eight such stations; and near future plans includes expansion to 24 cities. CDC quarantine inspectors are trained to recognize and report items and situations of public health significance, including illness in arriving passengers, and ensure that the appropriate medical and/or procedural action is taken.

- HHS is working with the U.S.-Mexico Border Health Commission and the Ministry of Health through a cooperative agreement to strengthen early warning disease surveillance capabilities in the six Mexican states bordering the United States. This Program is intended to enhance the infectious disease surveillance capabilities along the United States-Mexico Border by creating public health preparedness systems in the six Mexican Border States that are interoperable with one another and with those of the four United States Border States. This Program focuses on early detection, identification, and reporting of infectious disease outbreaks associated with potential bioterrorism agents or other major threats to public health.

- HHS is also contributing toward program development through cooperative agreements with the World Health Organization and the Pan American Health Organization, to enhance capabilities for

early detection, reporting, surveillance and response to infectious disease threats that might be related to bioterrorism.

- HHS/CDC maintains a network of laboratories designed to detect and respond to acts of biological and chemical terrorism known as the Laboratory Response Network (LRN). The LRN includes state and local public health, veterinary, military, and international labs. Canada, Mexico, Australia, and the United Kingdom are members of the network. Mexico was recently invited to join the network. HHS policy requires that LRN Members must use LRN approved laboratory test methods and reagents, and practice standard biosafety and biosecurity protocols.

*Controls On Financial Transactions, Assets and Services*

- The U.S. Department of the Treasury establishes and implements domestic controls to prevent the sourcing and distribution of illicit financial flows, including those that would enable and support proliferation activities.

*Bank Transactions*

- The U.S. Department of the Treasury administers the **Bank Secrecy Act (BSA)** through the Financial Crimes Enforcement Network (FinCEN). The BSA requires domestic financial institutions to maintain a financial trail on their customers' transactions, make reports to FinCEN, and to otherwise exercise due diligence when conducting those transactions.

- The BSA contains several important law enforcement tools that can be used to detect and deter the illicit trafficking of nuclear, chemical and biological weapons. FinCEN analyzes information under the BSA and identifies reports indicative of possible proliferation activity.[15] FinCEN then provides these reports along with supporting analyses to appropriate law enforcement agencies for further investigation.

*Suspicious Activity Reports*

- Chief among U.S. law enforcement tools is the requirement that banks, securities dealers, money services businesses, casinos, and certain other domestic financial institutions report suspicious activity. The dollar threshold for filing a suspicious activity report (SAR) generally is $5,000; the reporting threshold is even lower ($2,000) for point-of-sale activity involving certain smaller financial institutions, such as money transmitters. Congress also encouraged the voluntary filing of suspicious activity reports (even where the threshold is not met) by providing that financial institutions making voluntary filings are entitled to the same protection from civil liability as those making mandatory filings.[16]

*Cross-Border Cash Flow Reports*

- Financial institutions and individuals also are required to report the physical transportation of currency into or out of the United States. This cross-border movement of cash is reported to FinCEN on a currency and monetary instrument report (CMIR). The reporting dollar threshold is $10,000.[17]

*Record-Keeping*

- In addition to filing these reports with FinCEN, domestic banks and non-bank financial institutions are required to maintain a record of all funds transfers, domestic or international, involving more than $3,000. Identifying information about the originator and beneficiary of such funds transfers must be maintained for at least five years, and must be forwarded along with the payment order to the each succeeding financial institution in the payment stream. Similar recordkeeping requirements apply to the sale of monetary instruments for $3,000 or more in currency.

*Anti-Money Laundering Checks*

- Domestic financial institutions are also required to have anti-money laundering programs to assure compliance with the BSA regulations and to prevent their being used for money laundering and the financing of terrorism. These programs must include customer identification procedures for customers who open accounts; required procedures include both obtaining and verifying customer information to enable the financial institutions to form a reasonable belief that it knows the identity of its customer.

- Apart from the reporting, recordkeeping and due diligence requirements highlighted above, domestic financial institutions also may be subject to one or more of the special measures contained in **31 U.S.C. 5318A (as amended by section 311 of the USA Patriot Act)** for jurisdictions, financial institutions, or international transactions of primary money laundering concern. Those special measures include, among other things, additional reporting and recordkeeping obligations and prohibitions on the opening or maintaining of correspondent accounts.

*Due Diligence*

- Domestic financial institutions also are required to exercise due diligence concerning the opening or maintaining of correspondent accounts. These accounts are used by foreign financial institutions to conduct financial transactions in the United States. Correspondent accounts maintained on behalf of foreign banks operating in jurisdictions designated as non-cooperative with international anti-money laundering principles, designated as being of primary money laundering concern under 31 U.S.C. 5318A, or banks operating under an offshore license, are subject to special due diligence requirements. Similarly, they must have due diligence procedures

for private banking accounts maintained for foreign persons. These procedures must enable the financial institutions to monitor for and report transactions that appear to involve the proceeds of foreign corruption.

*Freezing Assets*

- Executive Order (E.O.) 13224 blocks all property and interests in property of foreign persons and entities designated by the President in the Order, or designated by the Secretary of State as committing, or posing a significant risk of committing, acts of terrorism, threatening the U.S. national security, foreign policy, or economy, if that property is either within the U.S. or within the possession or control of U.S. persons.

- E.O. 13224 also blocks the property and interests in property of persons determined by the Secretary of the Treasury to provide support or services to, or to be associated with, any individuals or entities designated under E.O. 13224. The Secretary of the Treasury may also block property and interests in property of persons determined to be owned or controlled by, or to act for or on behalf of, persons designated in or under the E.O. Any transaction or dealing by U.S. persons or within the U.S. in property and interests in property blocked pursuant to the Order is prohibited.

- U.S. law makes it a crime to provide material support or resources within the U.S. to a person intending that the support or resources will be used, or is in preparation for, the commission of a wide variety of specified terrorism-related crimes.[18] "Material support or resources" is very broadly defined and means "currency or other financial securities, financial services, lodging, training, expert advice or assistance, safe houses, false documentation or identification, explosives, personnel, transportation, and other physical assets, except medicine or religious materials."[19]

- In addition, U.S. law[20] prohibits the provision of "material support" to a Foreign Terrorist Organization.[21] A Foreign Terrorist Organization (FTO) may be designated pursuant to section 219 of the Immigration and Nationality Act.[22] When a financial institution becomes aware that it has possession of, or control over, any funds in which a Foreign Terrorist Organization, or its agent, has an interest, it shall retain possession or control over the funds, and report the existence of such funds to the Secretary of the Treasury. Failure to do so may result in civil penalties.

- Property provided as "material support" to a terrorist in violation of 18 U.S.C. § 2339A is subject to forfeiture if it is involved in a transaction or attempted transaction in violation of 18 U.S.C. § 1956-57, or if it is the proceeds of a section 2339A offense.[23] Providing prohibited "material support" is punishable criminally by 15 years imprisonment and/or fine of up to $250,000 for individuals and $500,000 for organizations.

*Law Enforcement*

- The FBI and ICE routinely develops and maintains appropriate effective law enforcement efforts to detect, deter, prevent and combat the illicit trafficking and brokering in such items. Where the investigation involves suspected terrorism links, the FBI coordinates its investigations with other federal law enforcement agencies and Intelligence Community members, and where necessary, with foreign counterintelligence and criminal investigative authorities.

- The FBI's capacity to conduct information collection under the Foreign Intelligence Surveillance Act has been enhanced through the passage of the USA Patriot Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001). Title III of the Patriot Act, known as the International Money-Laundering Anti-Terrorism Financing Act of 2001, provides the FBI with powerful anti-money laundering provisions for use in connection with its efforts to dismantle terrorist organizations and prevent future terrorist attacks. Provisions of this Act significantly erode the effectiveness of terrorist attempts to use: correspondent bank accounts, private bank accounts, offshore shell banks, and other criminal operations.

- A recent case highlights the FBI's use of various law enforcement and intelligence efforts to prohibit non-State actors from acquiring sensitive technology. Eased restrictions on contact between foreign counterintelligence and criminal investigative components of the Justice and Homeland Security Departments (facilitated by the Patriot Act) permitted the FBI to aggressively pursue foreign counterintelligence operations and criminal law enforcement actions against Philip Cheng, Howard Hsy and others, in connection with the proliferation of military technology.

- Philip Cheng, Martin Shih and Night Vision Technology (a corporate entity) have all been charged in the Northern District of California with conspiracy to violate the Federal Arms Export Control Act and the International Traffic in Arms Regulations and violations of the Federal Arms Export Control Act and the International Traffic in Arms Regulations. Shih has been charged with violation of the Export Administration Regulations of the United States and Cheng has been charged with money laundering.

- As leader of a government-wide effort to counter attempts to obtain state-of-the-art command, control, communications, computers, intelligence, surveillance and reconnaissance technologies, the FBI used declassified information gathered via intelligence techniques to obtain arrest warrants for seven subjects in Trenton, New Jersey, for exporting controlled military technology to countries of proliferation concern.

- The FBI has devoted considerable resources to the threat posed by WMD terrorism. To help counter the threat, a WMD Coordinator has been designated in each of the Bureau's 56 field offices. The WMD Coordinator serves as the WMD terrorism expert in each of the field offices and as liaison with state and local first responders. This individual receives additional training in the unique aspects of WMD investigations as well as on response to WMD threats and incidents.

*International Law Enforcement Cooperation*

- The United States has an extensive network of international cooperative arrangements and agreements that permit law enforcement authorities to exchange information, intelligence and evidence relating to trafficking in WMD weapons.
- The U.S. National Central Bureau (USNCB) of the International Criminal Police Organization (INTERPOL) transmits information on criminal justice, humanitarian, or other law enforcement matters between National Central Bureaus of INTERPOL member countries, and law enforcement agencies of the United States.
- In addition to both formal and informal arrangements at the policy level, the United States has numerous customs agreements as well as border inspection and pre-inspection arrangements. The United States also has a network of more than 50 bilateral mutual legal assistance agreements that may be invoked to provide assistance, including compulsory measures, to foreign authorities investigating or prosecuting criminal cases involving WMD proliferation. The United States has broad statutory authority to provide mutual legal assistance even in the absence of a treaty.
- By statute, CBP and ICE may share information and documents with foreign law enforcement agencies (19 U.S.C. 1628) if the exchange is necessary:
  - to ensure compliance with laws or regulations enforced by ICE or CBP;
  - to administer or enforce multilateral or bilateral agreements to which the U.S. is a party;
  - to assist in investigative, judicial, or quasi-judicial proceedings in the U.S.; or
  - to assist a foreign customs or law enforcement agency in an action comparable to the above, provided that the information will be held in confidence and used only for the purpose provided by ICE or CBP.
- To date, 53 Customs Mutual Assistance Agreements (CMAA) have been concluded with foreign governments for the exchange of such information.
- The Container Security Initiative is an initiative that was developed by the U.S. Customs in the aftermath of the terrorist attacks of September 11th. The purpose of CSI is to protect containerized shipping from terrorist activity and to prevent weapons of mass destruction (WMD) from arriving at U. S. ports. Now within the Department of Homeland Security, Customs and Border Protection (CBP) is continuing to implement CSI at major ports around the world. To date there are 25 ports operating with U.S. CSI teams performing targets.
- The Department of Energy's Second Line of Defense (SLD) Program's Megaport's Initiative complements the Container Security Initiative. By adding radiation detection capabilities at key ports, the United States will be providing host governments with the ability to screen container cargo for nuclear and radioactive materials that could be used against the United States, host countries, or allies.

- The United States has entered into a number of bilateral or multilateral agreements with other nations that provide a framework for cooperation in maritime law enforcement. Although such agreements have principally focused on the interdiction of illicit narcotics, illegal migrants, or terrorists, the United States is making interdiction of WMD a priority and is pursuing similar agreements with key flag states to address the proliferation of WMD, their delivery systems, and related materials by sea. These shipboarding agreements, concluded in support of the Proliferation Security Initiative (PSI), will facilitate the process of obtaining consent to board ships suspected of carrying cargoes of proliferation concern. The bilateral, reciprocal agreements provide for such things as information exchange, expedited confirmation of registry, jurisdiction, and procedures for obtaining authorization for defined law enforcement actions.

- The United States is presently engaged in multilateral negotiations at the International Maritime Organization (IMO) to amend the 1988 UN Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation (SUA), which applies to terrorist activities on ships. The proposed amendments would reach criminalize the transport of WMD, their delivery systems, and related materials by sea, as well as provide detailed shipboarding procedures.

*International Cooperation Related to Terrorist Financing*

- Led by the Treasury Department's Office of Terrorist Financing and Financial Crime (TFFC) the United States participates actively in the international Financial Action Task Force (FATF), various FATF style regional bodies (FSRBs), as well as many affiliated and in various subgroups including FATF's Working Group on Terrorist Financing (WGTF) and Typologies Working Group. The United States strongly supports eight special recommendations adopted by FATF in October 2001

    - Ratification and implementation of UN instruments;
    - Criminalizing the financing of terrorism and associated money laundering;
    - Freezing and confiscating terrorist assets;
    - Reporting suspicious transactions related to terrorism;
    - International Cooperation through mutual legal assistance or information exchange;
    - Alternative remittance systems;
    - Wire Transfers; and
    - The regulation and oversight of non-profit organizations

- Treasury continues to investigate other financing mechanisms used by terrorists to finance activities that include WMD proliferation, such as trade-based financing schemes and cash couriers. Treasury is conducting various international initiatives against illicit cash couriers in cooperation with FATF and the World Customs Organization (WCO). The United States supplies typologies and case studies to support the development of international standards on reporting, information sharing, and criminalization to combat illicit cash couriers.

- In its capacity as the United States' Financial Intelligence Unit (FIU), FinCEN participates in the Egmont Group, an international network of FIUs, representing 94 member countries, that share common goals, to enhance mutual cooperation and share information useful in detecting and combating money laundering and terrorist financing. The information collected by the Egmont Group FIUs has utility in detecting financing mechanisms associated with WMD proliferation, and the Egmont processes can sometimes significantly hasten and bolster multi-lateral information sharing.

***3(d). Establish, develop, review and maintain appropriate effective national export and trans-shipment controls over such items, including appropriate laws and regulations to control export, transit, trans-shipment and re-export and controls on providing funds and services related to such export and trans-shipment such as financing, and transporting that would contribute to proliferation, as well as establishing end-user controls; and establishing and enforcing appropriate criminal or civil penalties for violations of such export control laws and regulations;***

- U.S. law contains a variety of civil and criminal penalties for the unlicensed export, transit, trans-shipment or re-export of items or services related to nuclear, chemical or biological weapons.

- The U.S. Government requires licenses for the export of defense articles (which includes technical data) and defense services pursuant to the Arms Export Control Act (AECA), which prohibits the illicit transfer of U.S.-origin defense items to any unauthorized person. *See* 22 U.S.C. § 2778, and the implementing regulations, the International Traffic in Arms Regulations (ITAR), 22 C.F.R. Parts 120-130. Any person who violates any license, order or regulation issued pursuant to the AECA may be subject to civil fines, and those who willfully violate, or willfully attempt to violate any license, order or regulation issued pursuant to the AECA may be subject to criminal penalties including fines or imprisonment of up to 10 years.

- The U.S. Government also requires licenses for the export and re-export of sensitive U.S.- origin dual-use items and nuclear-related items consistent with the Department of Commerce's statutory and regulatory authorities for dual-use export controls (*see* Export Administration Act (EAA) of 1979, 50 U.S.C. App. §§ 2401-2420,[24] the Export Administration Regulations (EAR), 15 C.F.R Parts 730-799) and the export controls administered by the Nuclear Regulatory Commission (see Atomic Energy Act of 1954, 42 U.S.C. §§ 2011-2297q-4, and implementing regulations governing the export and import of nuclear equipment and materials, 10 C.F.R. §110.2).

- Any person who violates any license requirement, order or regulation consistent with the EAA or the Atomic Energy Act may be subject to civil fines. Those who willfully violate, or willfully attempt to violate any license requirement, order or regulation issued pursuant to the EAA or the Atomic Energy Act may be subject to criminal penalties including fines or imprisonment of up to 10 years, and 20 years in certain situations under the AEA.[25]

- Pursuant to E.O. 12938, if the Secretary of State determines a foreign person has contributed or attempted to contribute materially to the efforts of any foreign country, project, or entity of

proliferation concern to use, acquire, design, develop, produce or stockpile weapons of mass destruction or missiles capable of delivering them, the measures specified in E.O. 12938 are to be imposed on that foreign person to the extent determined by the Secretary of State in consultation with certain agencies. The measures include a procurement ban on U.S. Government procurement of goods, technology, or services from the designated foreign person; an assistance ban on any U.S. Government assistance to the designated foreign person); and an import ban.

- Implementation of the import ban is delegated to the Secretary of the Treasury. E.O. 12938 provides that the Secretary of the Treasury shall prohibit the importation into the United States of goods, technology, or services produced or provided by the designated foreign persons on which the Secretary of State has determined to impose an import ban. (Information or informational materials within the meaning of § 203(b)(3) of the International Emergency Economic Powers Act (IEEPA), 50 U.S.C. 1702(b)(3), are exempt from this prohibition.) The Regulations, in turn, implement the import ban.

- A civil penalty not to exceed $11,000 per violation may be imposed on any person who violates or attempts to violate any license, order or regulation issued under the IEEPA. Whoever willfully violates or willfully attempts to violate any license, order, or regulation issued under the Act, upon conviction, shall be fined not more than $50,000, and if a natural person, may also be imprisoned for not more than 10 years; and any officer, director, or agent of any corporation who knowingly participates in such violation may be punished by a like fine, imprisonment, or both. The criminal penalties provided in the act are subject to increase pursuant to 18 U.S.C. 3571.

- Other administrative sanctions may also be imposed for a violation of U.S. export controls, including the suspension or revocation of export privileges under 15 C.F.R. § 764.3(a)(2); and 15 C.F.R. § 720 (denial of export privileges under the Chemical Weapons Convention Regulations).

- Administrative enforcement proceedings take place before an administrative law judge, and the party accused of a violation may mount a legal defense. Under 15 C.F.R. § 766, these respondents are entitled to, among other things, notice of the charges being brought against them, an opportunity to answer or otherwise respond to those charges, an opportunity to obtain information from the Commerce Department relevant to any claim or defense in the proceeding, and an opportunity for a hearing before the administrative law judge.

- Another approach that is often available in export control cases is to prosecute persons or entities for making false statements to the federal agencies and departments which exercise the licensing authority over the export of controlled items or services, such as false representations in a Shipper's Export Declaration or other shipping or export forms submitted to the agencies, which violates either the general false statements statute (18 U.S.C. § 1001) or a specific false statement offense found in the export control statutes or in the implementing regulations.

- *Recent prosecutions for export violations concerning WMD technology include:*

  - *On Sept. 23, 2003, Omega Engineering of Stamford, Connecticut, was sentenced to pay $313,000 in criminal fines and an $187,000 civil penalty. On Sept. 22, the Chief Financial Officer of Omega was sentenced to 5 years imprisonment and 5 years home confinement. The sentences resulted from an ICE investigation, which found that Omega and its CFO had willfully disregarded the denial of a U.S. export license, and illegally exported laboratory equipment with nuclear and non-nuclear applications to the Pakistani Ministry of Defense, National Development Center.*

- *Money laundering and asset forfeiture provisions also cover export control offenses:*

  - *U.S. law provides that Specified Unlawful Activity (SUA) includes criminal violations of Section 38(c) of the AECA, section 11 of the EAA, and section 206 (relating to penalties) of the IEEPA (see* 18 U.S.C. §1956(c)(7)(D)).

  - Additionally, a violation of *another country's* export control laws can also constitute a money laundering offense. In other words, if a person conducts or attempts to conduct a financial transaction occurring in whole or in part in the United States, where the person knows the transaction involves proceeds related to a prohibited export or re-export of controlled items, this is a violation of U.S. money laundering laws. (see 18 U.S.C. §1956(c)(7)(B)(v)(I) and (II)).

  - Any property, real or personal, involved in a violation of 18 U.S.C. §§1956 and 1957 (involving violations of the AECA, EAA or their foreign counterpart or the IEEPA), or any property derived from, traceable to such property or any property used to facilitate such an offense, is subject to civil and criminal forfeiture pursuant to 18 U.S.C. §§ 981 and 982.

- Prosecutorial resources dedicated to the export control area:

  - The Counterespionage Section of the Department of Justice's Criminal Division includes attorneys with experience in the prosecution of export control offenses. These attorneys also regularly provide training on export control law to prosecutors in the U.S. Attorney's Offices and to investigators with the Departments of Commerce and Homeland Security (ICE). The Counterespionage Section has drafted a monograph concerning the export control laws and maintains a list of significant export control cases, both of which it disseminates to assist prosecutors and investigators in the field.

  - Additionally, each U.S. Attorney's Office has a national security coordinator who regularly receives training in export control laws.

*NRC Administers Controls On Exports and Imports of Nuclear Material and Equipment*

- The U.S. Nuclear Regulatory Commission (NRC) is responsible for establishing and enforcing regulatory controls over exports or imports of nuclear materials, facilities and equipment pursuant to the requirements of the AEA as amended by the Nuclear Non-Proliferation Act of 1978.[26]

- The AEA establishes required NRC review procedures including obtaining judgments from interested Executive Branch agencies (Departments of Commerce, Defense, Energy, and State) as to whether specific export licensing criteria are satisfied. The level of reviews and stringency of the criteria correspond to the perceived nuclear proliferation or explosive risk posed by materials, facilities or equipment involved. NRC regulations setting forth the levels of review and criteria governing approval of exports and imports of the various types of nuclear materials, facilities and equipment under NRC jurisdiction are found in 10 CFR Part 110.

- NRC regulations in 10 CFR Part 110 establish two types of NRC export/import licenses depending largely on the risk significance of the nuclear materials or equipment involved. A general license for certain low-risk materials is effective without the filing of a specific application with NRC and without the issuance of a license document to a particular person. A specific license is effective only after a company with a permanent U.S. address files an application with NRC for review and a license ("piece of paper") is issued if relevant criteria are met.

- NRC forwards applications requiring Executive Branch review to the Department of State, the Agency designated as coordinator of that process. The Executive Branch is asked to provide its judgment on relevant criteria including whether approval of a proposed export would be inimical to the common defense and security of the U.S.

- If, after receiving a favorable Executive Branch judgment and considering other available information, the NRC determines the relevant criteria are met, it will issue the license. If, after receiving favorable Executive Branch views NRC is unable to determine that relevant criteria to issue a license are met, the application including the results of the review would forwarded to President of the United States to decide the outcome.

- Violations of NRC regulatory requirements for exports and imports of nuclear materials and equipment are subject to criminal penalties administered by the Department of Justice or civil penalties administered by NRC.

- Following the terrorist attacks in the United States on September 11, 2001, NRC and other U.S. Government agencies engaged in a variety of domestic and international reviews focusing in particular on the potential for certain high-risk radioactive materials to be used in a radiological dispersion device. These efforts resulted in a major revision to the IAEA Code of Conduct on the

Safety and Security of Radioactive Sources (Code of Conduct) providing guidance for the adoption of policies and laws to ensure that such sources are not diverted for illicit use.

- As a result of these efforts, NRC concluded that it is essential to update and enhance domestic export/import licensing requirements for high-risk radioactive sources to protect public health and safety and to be consistent with international guidelines. Accordingly, the proposed revisions to NRC export/import regulations recently published for public review and comment would establish requirements for the issuance of specific licenses for exports and imports of specified high risk sources to ensure that recipients are legitimately authorized entities.

*Department of Energy Controls on Exports of Nuclear Technology and Other Transfers*

- Under Section 57b of the Atomic Energy Act of 1954, as amended, it is unlawful for any person to engage directly or indirectly in the production of special nuclear material (plutonium or enriched uranium) outside the United States, except as authorized by the Secretary of Energy or otherwise provided by law. Department of Energy (DOE) regulations 10 CFR Part 810 govern exports of nuclear technologies and services. To authorize such an export, the Secretary of Energy must have the concurrence of the Department of State and must consult the Departments of Defense and Commerce and the Nuclear Regulatory Commission. Controls on nuclear technology transfers, as well as reviews on items subject to Department of Commerce, Department of State, or Nuclear Regulatory Commission licensing jurisdiction, are administered by the National Nuclear Security Administration's Office of Export Control Policy and Cooperation.

- The Part 810 regulations reflect U.S. obligations as a member of the Non-Proliferation Treaty, as well as U.S. commitments undertaken in the Nuclear Exporters Committee (Zangger Committee) and the Nuclear Suppliers Group, as well unilateral U.S. nonproliferation controls.

- The regulations contain a list of countries requiring the Secretary's specific authorization for virtually all exports of nuclear technology and services, including exports relating to civil nuclear power reactors and fuel. The Part 810 list comprises all countries posing nuclear proliferation or national security concerns and all countries that do not have a full-scope safeguards agreement with the International Atomic Energy Agency (IAEA) in effect.

- The regulations require specific authorization by the Secretary for exports to all countries of technology and services related to production reactors; uranium enrichment; plutonium reprocessing; accelerator-driven sub-critical assemblies; fabrication of fuel containing plutonium; heavy water production; or research or test reactors capable of continuous operation greater than five megawatts thermal.

- When specific authorizations are approved, DOE requires assurances from the recipient government that no transferred U.S. technology or services will be used for any military purpose and none will be retransferred to another country without prior U.S. Government consent.

- The regulations provide general authorization for certain specific activities including exports of nuclear technology and services to civil nuclear power reactors and fuel to countries that are not on the Part 810 list; furnishing public information; assistance in radiological emergencies; enhancing operational safety of existing reactors provided notice is given to the DOE, implementing the U.S.-IAEA Safeguards Agreement; participating in approved IAEA programs; participating in exchange programs approved by the Department of State in consultation with DOE; and participating in open meetings sponsored by scientific, technical, or educational organizations.

- DOE requires U.S. nuclear vendors to obtain advance approval for hiring foreign nationals who may acquire nuclear technologies in the course of their employment. In performing such reviews, DOE considers possible proliferation concerns posed by the foreign national. DOE also may advise the U.S. firm to consult the Department of Commerce on whether a "deemed export" license is required.

*The Department of Commerce Administers Dual-Use Export Controls*

- The Department of Commerce controls exports of dual-use items, which are commercial items that while not designed as weapons, delivery systems, or for terrorist purposes, have the potential for this type of misuse. The Department of Commerce is responsible for controlling sensitive items identified on the Commerce Control List (CCL), which the United States considers to be of significant value to the development, testing, deployment, and delivery of Weapons of Mass Destruction (WMD) and other military programs of concern. Certain items on the CCL may require a license for export to all destinations while other items may be eligible for a license exception if intended for a close ally or partner.

- The Department of Commerce in conjunction with the Department of Justice conducts civil and criminal investigations of violations relating to dual-use export controls. The U.S. Government may impose civil, administrative, or criminal sanctions for dual-use export controls violations under the authority of the International Emergency Economic Powers Act (IEEPA), as amended, (50 U.S.C. §§ 1701-1706), and consistent with the Export Administration Act of 1979, as amended (EAA) (50 U.S.C. app. §§ 2401-2420), the Export Administration Regulations (EAR) (15 C.F.R. Parts 730-774) and the Chemical Weapons Convention Implementation Act of 1998 (CWCIA) (22 U.S.C. §§ 6701-6771).

- The Department of Commerce also enforces industry compliance with the Chemical Weapons Convention export controls requirements, reviews visa applications of foreign nationals to help prevent illegal technology transfers; ensures compliance with export license conditions through end-use inspections; and conducts cooperative enforcement activities with foreign counterparts.

- Department of Commerce special agents have traditional police powers, including the authority to make arrests, execute warrants, issue administrative subpoenas, and detain, seize, and forfeit goods. Commerce investigators are posted to major technology export centers throughout the

country: Los Angeles, California; San Jose, California; New York City, New York; Herndon, Virginia; Boston, Massachusetts; Miami, Florida; Dallas, Texas; Houston, Texas; and Chicago, Illinois. Special agents at Commerce headquarters in Washington, D.C. collect and analyze information regarding potential dual-use export control violations.

- The Department of Commerce also undertakes preventive enforcement measures by reviewing shipments exported under license exceptions and conducting pre-license checks and post-shipment verifications for licensed transactions. Commerce and Department of Homeland Security special agents conduct joint investigations and enforcement projects.

*The Department of Commerce Dual-Use Export License Process*

- Under the EAR (15 C.F.R. Part 732), exporters may be required to submit a license application for an export or re-export of a U.S. origin dual-use item depending on an item's technical characteristics, the destination, the end-user, and the end-use. If after reviewing the EAR (15 C.F.R. Part 748) an exporter determined a license was required, the exporter would submit a license application.

- Exporters may submit license applications through an electronic system called the Simplified Network Application Process (SNAP) system.

- The Department of Commerce licensing officers review and analyze license applications along with documentation submitted in support of the applications. Licensing officers will assess the item, its destination, its end-use, and the reliability of each party to the transaction in making a decision to approve or deny the license application. Commerce may return an application without action if it is determined that no license is required for the transaction or more information is needed to process the application. Commerce also refers export license applications for review to the Departments of State, Energy, and Defense. (15 C.F.R. Part 750). Processes exist to obtain interagency consensus on whether to approve or deny a license application. Commerce also consults with the intelligence community in making licensing decisions.

- In calendar year 2003, Commerce received 13,637 dual-use export license applications and completed 13,465. 11,285 were approved, 251 denied, 1,928 returned without action and one was suspended/revoked. The average processing time for all license applications was 42 days, with 44 days for applications referred to other agencies and 14 for applications not referred.

*Deemed Export Controls*

- Also under the EAR (15 C.F.R. 734.2(b)(2)(ii)), the Commerce Department administers export licensing of dual-use technology transfers to foreign nationals in the United States. Transfer of controlled technology to a foreign national is "deemed" to be an export to the foreign national's home country. If the controlled technology would require a license for a direct export to that foreign national's home country, then a "deemed" export license is required for a foreign national

to have access to that technology here in the United States. The vast majority of "deemed" export licenses are for foreign nationals on H1B working visas that require access to controlled technology because of their employment. The foreign national's employer is required to submit a license application and have that application approved before the foreign national can have access to controlled technology.

*"Catch-all" Export Controls*

- Under 15 C.F.R. Part 744, the United States implements "catch-all controls," that require exporters to obtain a license to export any U.S.-origin item, even a non-controlled item, if they know or are informed that the item will be used in or by certain countries for prohibited nuclear activities, chemical or biological weapons programs, or the design, development, or production of missiles, or in facilities engaged in such activities.

- In addition, catch-all controls extend to the activities of U.S. persons. Under the EAR (15 C.F.R. Part 744.6), U.S. persons may not perform any contract, service, or employment knowing it will directly assist in chemical and biological weapons or missile activities in or by certain countries.

- The United States is currently strengthening its national missile technology and chemical/biological catch-all controls by applying catch-all controls on a global basis. Strengthened controls, by virtue of this global approach, will apply to terrorists and other non-state actors such as illicit traffickers and brokers. The United States is also developing a terrorism catch-all policy that will prohibit the export or re-export of U.S.-origin items where the exporter knows the item will be used for a terrorism end-use.

*Restrictions on Exports to Specific End-Users and End-Uses*

- The EAR (15 C.F.R. Part 744.2, 744.3, 744.4, 744.5) generally prohibit exports and re-exports of items subject to the EAR to certain nuclear, missile, chemical, and biological activities and nuclear maritime end-users and prohibits other actions in support of such activities.

- U.S. export controls also restrict exports to specific end-users, such as terrorists (15 C.F.R. Part 744.12, 744.13, 744.14). The EAR prohibit exports and re-exports of any items to persons designated by the Department of Treasury for terrorism reasons. These controls are intended to prevent acts of terrorism and to affirm U.S. opposition to international terrorism by limiting the ability of designated terrorist organizations and individuals to obtain and use U.S.-origin items in terrorist operations.

- More generally, the EAR (15 C.F.R. Part 744, Supplement No. 4) contain an Entity List that identifies specific end-users in countries throughout the world that pose a proliferation concern. Many of these end-users have been listed because of missile proliferation concerns. For most end-users identified on the Entity List, a license is required for all exports subject to the EAR.

- The Department of Commerce also maintains on its website an informal listing of persons for whom the United States has denied their export privileges. See http://www.bis.doc.gov/dpl/Default.shtm No export licenses may be granted to a denied person nor may other exporters participate in transactions with a denied person without Department of Commerce authorization. This is an important tool that allows the Commerce Department to restrict export privileges for these actors and prohibit others from participating in transactions with them.

*Review and Maintenance of Appropriate Effective National Export Controls on Dual-Use Items*

- The United States' Commerce Control List (CCL) is reviewed systematically in the context of the multilateral export control regimes, which periodically evaluate multilateral dual-use export control lists that provide the foundation for the CCL. (See Para 6 of this report for a description of the list.) U.S. interagency working groups such as the Missile Annex Review Committee (MARC) and Subgroup on Nuclear Export Coordination (SNEC) determine the necessity for and parameters of control for specific items.

***6. Recognizes the utility in implementing this resolution of effective national control lists and calls upon all Member States, when necessary, to pursue at the earliest opportunity the development of such lists;***

*United States National Control Lists*

- Commerce Control List (Dual-Use): The foundation for U.S. dual-use export controls is the Commerce Control List, known as the CCL. Dual-use commodities are commercial items that, while not designed as weapons, delivery systems, or for terrorist purposes, have the potential for this type of misuse. The Commerce Control List is authorized by the Export Administration Act of 1979, as amended, Section 4(b), and is implemented by regulation in 15 C.F.R. Part 774. The CCL is consistent with control lists agreed to in the multilateral context, such as the Wassenaar Arrangement, Nuclear Suppliers Group, Australia Group, and Missile Technology Control Regime. As revisions are made to the multilateral control lists, revisions are also made to the CCL.

- In addition, the U.S. Government has created a listing of foreign end-users involved in proliferation activities. The Department of Commerce maintains the Entity List to provide notice informing the public of export license requirements related to these entities. (15 C.F.R. Part 744, Supplement No. 4). While an export or re-export license is required for most exports and re-exports to these entities, the licensing policy varies depending on the end-use or end-user as well as the nature of the item.

- Munitions Control List: United States Munitions List: The United State Munitions List (USML) consists of twenty-one broad categories of defense articles and services that are subject to the International Traffic in Arms Regulations (ITAR) (22 CFR 120-130). Items may be controlled

under the ITAR if they: (1) are specifically designed, developed, configured, adapted, or modified for a military application, and (2) do not have a predominant civil application, and (3) do not have a performance equivalent (defined by form, fit and function) to those of an article or service used for civil application. Alternatively, an article or service may controlled if it is specifically designed, developed, configured, adapted, or modified for a military application, and has significant military or intelligence capability to warrant control.

- The President's authority under the terms of Section 38 of the Arms Export Control Act (AECA) (22 U.S.C. 2778) to designate defense articles and services is delegated to the Secretary of State by Executive Order 11958, as amended. This authority is the basis for the Department of State's responsibility to license the permanent and temporary export and the temporary import of defense articles and services. With few exceptions provided for in U.S. law and regulation, all exports of defense articles or services require a license. Licensing is performed on a case-by-case basis in accordance with the ITAR, which includes the USML as Part 121, and which are promulgated under the delegated authorities of the AECA. Defense articles generally are licensed for use by state entities such as Ministries of Defense or law enforcement authorities, though some defense articles and services may be licensed to non-state actors (e.g., defense manufacturers) with established bona fides. All parties to an export transaction are checked against a watchlist and may be subject to pre-license and post-shipment checks. Any change in end-use or retransfer to a third party other than approved in a license requires the prior written approval of the Department of State.

- Select Agents List: Biological Materials: The United States has established, by regulation, lists of biological agents and toxins determined to have the potential to pose a severe threat to human health, animal or plant health, or to animal and plant products. These regulations require all persons possessing, using, or transferring these biological agents and toxins to register with either the Secretary of Health and Human Services, or the Secretary of Agriculture, or both.

- HHS regulations implementing the Bioterrorism Act (known as the "Select Agent regulations"), became effective on February 7, 2003, and fully applicable on November 12, 2003. Select agents are identified at 42 C.F.R. § 73.4 (HHS select agents and toxins) and 42 C.F.R. § 73.5 (Overlap select agents and toxins). The Select Agent regulations include requirements concerning registration of persons possessing select agents and toxins, safety, security plans, and emergency response plans, training, transfers of select agents, record keeping, inspections, and notifications of theft, loss, or release.

- Under the authority of the Agricultural Bioterrorism Protection Act of 2002, the Secretary of Agriculture published parallel Select Agent regulations in 7 C.F.R. Part 331 and 9 C.F.R. Part 121. While the focus of the HHS regulations was on the potential of a biological agent or toxin to pose a severe threat to human health, the focus of the USDA regulations was on its potential to pose a severe threat to animal, plants, and animal and plant products.

- In addition to establishing national control lists of goods, the United States also takes action to target individuals and/or entities of concern to prevent them from acquiring goods and technology.

*Designation of Specially-Designated Nationals (SDN) and Foreign Terrorist Organizations (FTO)*

- Under Section 219 of the Immigration and Nationality Act[27] (as amended by the Anti-terrorism and Effective Death Penalty Act of 1996), the Secretary of State may, in consultation with the Attorney General and the Secretary of the Treasury, designate an organization as a Foreign Terrorist Organization (FTO) if the organization is a "foreign organization", that "engages in terrorist activity" that "threatens the security of U.S. nationals or the security of the United States". The Department of the Treasury may require U.S. financial institutions possessing or controlling assets of designated FTOs to block all financial transactions involving these assets.

- Under E.O. 12947 of January 23, 1995, as amended by E.O. 13099 of August 20, 1998, the President designated sixteen organizations, and authorized the Secretary of State to designate additional foreign individuals or entities who have committed, or pose a significant risk of committing, acts of violence with the purpose or effect of disrupting the Middle East Peace Process, or who have provided support for or services in support of such acts of violence.

- E.O. 12947 further authorizes the Secretary of the Treasury to block the property of persons determined to be owned or controlled by, or acting for or on behalf of, persons designated in or under the Order. All property and interests in property of persons designated under the Order in the U.S. or in the control of U.S. persons are blocked. Any transaction or dealing in such blocked property is also prohibited.

- OFAC publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. Collectively, such individuals and companies are called "Specially Designated Nationals" or "SDNs." Their assets are blocked and U.S. persons are generally prohibited from dealing with them. See http://www.treas.gov/offices/enforcement/ofac/sdn The list also includes individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific.

- E.O. 13224 provides the U.S. Government with a mechanism to block designees' assets in any financial institution in the United States or held by any U.S. person as well as to require the blocking of any transactions. E.O. 13224 also permits the designation of individuals and organizations that provide support or financial or other services to, or associate with, designated terrorists. The designation authority under E.O. 13224 combined with U.N. Security Council Resolutions (1267/1337/1373/1390/1455) are key components in the international effort to freeze the assets of terrorist supporters.

- The publication of SDNs provides actual notice of actions by OFAC with respect to Specially Designated Nationals and other persons whose property is blocked, in an effort to assist the public

in complying with the various sanctions programs administered by OFAC. Users are advised to check the *Federal Register* and the SDN list routinely for the most current version of the list.

- Entities and individuals on the list are occasionally licensed by OFAC to transact business with U.S. persons in anticipation of removal from the list or because of foreign policy considerations in unique circumstances. Licensing in anticipation of official *Federal Register* publication of a notice of removal based on the unblocking of an entity's individual property is reflected in this publication by removal from the list.

7. ***Recognizes that some States may require assistance in implementing the provisions of this resolution within their territories and invites States in a position to do so to offer assistance as appropriate in response to specific requests to the States lacking the legal and regulatory infrastructure, implementation experience, and/or resources for fulfilling the above provisions;***

- Through various U.S. assistance programs, the United States works with countries globally to develop legal and regulatory infrastructure, implementation experience, and/or resources to fulfill the provisions outlined in the resolution through bilateral programs and as an active participant in multilateral programs.

*Training: Financial Crimes/Money Laundering*

- The U.S. Department of Justice plays a major role in assisting states to develop legislation and regulations to criminalize the financing of terrorism and terrorist acts which can include the acquisition and use of weapons of mass destruction. Justice also responds to states' requests for expertise and training to help develop their professional skills and capacity to implement these laws and to prosecute and adjudicate such crimes.

- The United States Department of Treasury does extensive outreach to support the global fight against terrorist financing, including encouraging nations to remove the legal or other barriers that might hinder cooperative efforts. The Department of Treasury also responds to requests for technical assistance to block terrorist assets, cut off terrorist fund flows, and prevent fund-raising activities that benefit terrorists. This may include activities focused on acquisition of weapons of mass destruction or related materials.

- The United States assists in criminal investigations or proceedings related to terrorist acts and their support activities, including financing schemes, through bilateral programs and as an active participant in multilateral programs. The U.S. Department of Treasury and Department of Justice provide training and technical assistance on financial investigations to foreign law enforcement, regulatory and prosecutorial counterparts.

- Additionally, the Internal Revenue Service (IRS-CI) has seven law enforcement attachés assigned to American Embassies or U.S. Consulates in Mexico City, Bogotá, London, Frankfurt,

Bridgetown, Ottawa, and Hong Kong. These attachés help with financial investigations, terrorist financing matters, international training and technical assistance.

- The IRS also provides technical assistance to foreign governments to help develop criminal, tax, and financial investigation organizations.

- Since September 11, 2001, the Department of Justice has provided assistance to several countries to assess their money laundering laws, policies and procedures. Follow-up training in anti-money laundering / anti-terrorism financing techniques has been conducted in the Bahrain, Brazil, Colombia, the Cook Islands, Kenya, Kuwait, Malaysia, Oman, Pakistan, Paraguay, Panama, the Philippines, Qatar, Thailand, Turkey, and the United Arab Emirates. Additional courses will be conducted over the coming year in Bangladesh, the Czech Republic, Egypt, Indonesia, Kazakhstan, Nepal, and Saudi Arabia.

- The United States also sponsors the International Law Enforcement Academies (ILEA's) in Botswana, Hungary, Thailand and an advanced academy in Roswell, New Mexico, USA. The Department of State is currently exploring a venue for a potential ILEA in Latin America. Senior representatives from the Departments of State, Treasury, Justice and Homeland Security comprise the ILEA Policy Board, which performs monitoring activities and provides overall guidance and oversight of the training program to ensure that it is consistent with foreign policy and law enforcement goals. An Interagency Steering Group provides operational guidance. Participating agencies include DOS, ATF, DOJ, INS, FBI, DEA, ICE, IRS-CI, DHS' Federal Law Enforcement Center (FLETC), DOS – Diplomatic Security Services and others. The Department of State maintains a website for ILEA relative to their Academies: http://www.state.gov/g/inl/ilea/.

*WMD Materials Security and Control*

- The Departments of Defense and Energy work bilaterally and multilaterally with many countries worldwide to **detect, prevent, and reverse the proliferation of weapons of mass destruction. Many of these programs strengthen the domestic security of the nuclear complexes and proliferation-sensitive materials in other countries. These efforts include:**
  - **Securing nuclear materials, nuclear weapons and radiological materials at potentially vulnerable sites in Russia and elsewhere;**
  - **Reducing quantities of nuclear and radiological materials;**
  - **Bolstering border security overseas with training and nuclear detection capabilities;**
  - **Strengthening international nonproliferation and export control regimes;**
  - **Downsizing the nuclear weapons infrastructure of the former Soviet Union**

- The Strategic Offensive Arms Elimination (SOAE) Program in Russia provides equipment and services to destroy or dismantle ICBMs, ICBM silo launchers, road and rail mobile launchers, SLBMs, SLBM launchers and associated SSBNs, and related infrastructure in accordance with the START Treaty. The program also supports the disposition of spent naval reactor fuel from dismantled SSBNs.

- The Chemical Weapons Destruction (CWD) Program assists Russia in the destruction of its nerve agent stockpile and in the demilitarization of former CW production facilities.

- The Strategic Nuclear Arms Elimination (SNAE) Program in Ukraine has achieved its denuclearization goals for Ukraine. Other assistance includes the elimination of Tu-22M Backfire nuclear-capable bombers and Kh-22 nuclear air-to-surface missiles. The U.S. Department of Defense also has offered to support elimination of all 163 SS-24 loaded motor cases by either open detonation or open burning.

- The Weapons of Mass Destruction Infrastructure Elimination (WMDIE) Program in Ukraine assists with the elimination of nuclear weapon storage sites. The WMDIE Program in Kazakhstan assists with the destruction of WMD-related infrastructure and has worked to dismantle facilities at the former anthrax production facility at Stepnogorsk.

- The Biological Weapons Proliferation Prevention (BWPP) Program assists states of the former Soviet Union to reduce the proliferation risk from biological weapons technology, pathogens and expertise. Four integrated project areas under the BWPP Program work toward this end: Cooperative Biological Research (CBR), Biological Threat Agent Detection and Response (TADR), BW Infrastructure Elimination, and Biosecurity/ Biosafety (BS&S).

- The Nuclear Weapons Storage Security (NWSS) Program in Russia enhances the security, safety, and control of nuclear weapons during storage. It also assists Russia with drug and alcohol screening and evaluation of personnel who have access to nuclear weapons and improves the safety of those personnel by providing dosimeters for radiation and radon detection.

- The Nuclear Weapons Transportation Security (NWTS) Program in Russia supports proliferation prevention objectives by enhancing the security, safety, and control of nuclear weapons during shipment.

- The Fissile Material Storage Facility (FMSF) Program in Russia provides a centralized, safe, secure, and ecologically sound storage for fissile material removed from nuclear weapons, and enhances material control, accounting, and transparency, which increases confidence that the stored weapons grade fissile material is safe and secure, and that the fissile material declared excess to military needs will not be reused for nuclear weapons.

- The WMD Proliferation Prevention Initiative (WMD-PPI) for non-Russian FSU states assists Azerbaijan, Kazakhstan, Uzbekistan, and Ukraine in strengthening their ability to deter, detect, and interdict trafficking of WMD and related materials.

- Defense and Military Contacts projects expand contacts between defense establishments to promote objectives that include stemming the proliferation of FSU WMD.

- The Department of Energy helps develop national and regional resources in Russia to support effective operation of upgraded nuclear material protection, control and accounting (MPC&A) systems. DOE is also developing strategies to transition technical and financial support for MPC&A systems to the Russian Federation. These projects include MPC&A regulations development, Atomic Energy (FAAE) inspections, tracking nuclear materials inventories, training for physical protection and material control and accounting operations, and for maintenance of the MPC&A Operations Monitoring (MOM) system, equipment certification and vendor support, transportation security, and protective force enhancement.

- The Global Nuclear Material Threat Reduction program removes vulnerable nuclear material; reduces and, to the extent possible, eliminates HEU from civil applications worldwide. Under this program, the Department of Energy will conduct multi-year initiatives to: (1) return to the United States U.S-origin spent nuclear fuel from foreign research reactors in 40 countries, (2) return to the Russian Federation 4 MT of both fresh and irradiated Soviet-/Russian-supplied fuel, (3) convert 105 targeted research reactors from the use of HEU fuel to the use of LEU fuel, (4) convert the use of HEU targets to the use of LEU targets in the production process for molybdenum-99, (5) secure for final disposition three tons of weapons-grade plutonium contained in spent nuclear fuel from the BN-350 fast breeder reactor in Kazakhstan, and (6) remove other vulnerable nuclear material not currently covered by existing programs.

- Under the Global Radiological Threat Reduction program the United States will conduct multi-year initiatives to improve security at 299 sites worldwide containing high risk radiological sources; recover and dispose of sources from 800 radioisotope thermal electric generators (RTGs); and recover over 20,000 at-risk radiological sources within the United States within the next decade.

- The Nonproliferation and International Security program is intended to prevent, detect and reverse proliferation of WMD material and technology as well as strengthening the nonproliferation regime. Under this program, the Department of Energy is conducting multi-year initiatives to: (1) secure materials through security upgrades at civilian reactors in 54 countries; (2) reverse WMD programs, including removal of material and equipment from countries such as Libya and Iraq; (3) review more than 4,000 export license applications annually; (4) strengthen the nonproliferation regime by training 13,000 IAEA inspectors, export control officials and other nonproliferation experts by 2013; (5) strengthen export control regimes in 36 emerging suppliers, FSU and transshipment states; and (6) conduct six technology exchanges on the safety and security of nuclear warheads with Russia and other countries annually.

- The International Material Production and Cooperation program improves the security of weapons-usable nuclear and radiological material and enhances detection and interdiction infrastructure at international borders. Working with Russia and countries of the former Soviet Union, the program helps secure nuclear weapons and weapons-usable nuclear materials by upgrading security at nuclear sites, consolidating these materials to sites where installation of

enhanced security systems have already been completed, and improving nuclear smuggling detection capabilities at border crossings.

- The Russian Transition Initiative prevents the migration of WMD expertise from the former Soviet weapons complex. Under this program, the Department of Energy conducts multi-year programs, which have to date engaged over 16,500 former weapons scientists, engineers, and technicians in enterprise development and technology commercialization; downsizing workforce and facilities at 6 Russian nuclear weapons sites; and leverage funding from private industry contributions or other non-USG sources equal to 100% of program funds.

- As part of United States' efforts to dispose of surplus weapons-usable fissile materials, the Department of Energy's National Nuclear Security Administration (NNSA) will design, build and operate facilities to dispose of 34 metric tons of surplus U.S. weapons-grade plutonium as well as work with Russia to dispose of similar quantities of surplus Russian weapons-grade plutonium. The NNSA is also overseeing the disposition of 174 metric tons of U.S. surplus highly enriched uranium.

- The Department of Energy, through its program on ending weapons-grade plutonium production (EWWGPP) in Russia, will provide assistance for the construction or refurbishment of fossil-fueled plants to replace the last three aging plutonium production reactors still operating in Russia. This program will enable the complete shutdown of these reactors and this the capping of new production of weapon-grade plutonium, while measures under the U.S.-Russian Plutonium Production Reactor Agreement (PPRA) will continue to monitor all plutonium produced by these reactors since 1995, to ensure it is secure, accounted for, and never again used in weapons.

- The United States provides training, technical assistance and equipment through the Department of State's Export Control and Related Border Security Assistance (EXBS) program to assist countries to develop strong export and border control systems to prevent the proliferation of Weapons of Mass Destruction (WMD), their missile delivery systems, advanced conventional weapons, and related items. The EXBS program works with governments in strengthening their export controls by improving their legal and regulatory frameworks, licensing processes, border control and investigative capabilities, outreach to industry, and interagency coordination. The Department of State implements the EXBS program in over 40 countries by drawing on expertise from the Departments of Commerce, Energy, and Homeland Security and from the private sector. The program also has placed over 20 Program Advisors at U.S. Embassies to help to coordinate and implement assistance.

- In support of the Department of State-lead EXBS program, the Department of Commerce conducts technical exchanges designed to remedy deficiencies that the U.S. Government has noted in certain dual-use national export control systems. Commerce has conducted over 400 technical exchanges in 33 countries and has identified and remedied 323 deficiencies. Identified deficiencies range from the non-existence of an export control law to a control list that does not conform to international regime standards.

- The Department of Justice, working closely with the Department of State and the EXBS program, will commence work in Asia in 2005, assessing both the legislative and regulatory frameworks for criminalizing the use of weapons of mass destruction for terrorist acts, and the ability of law enforcement institutions and specialized agencies to effectively investigate and prosecute such acts. Based on the assessments, the Department of Justice would then provide technical assistance, such as legislative drafting, skills building for investigators, prosecutors, and judges, and implementing new laws and regulations.

- Via a customized software program called TRACKER, the United States helps other countries' export control officials network via a standardized database with licensing officials in other countries.

- The Science Centers program, coordinated by the Department of State, provides former weapons scientists with opportunities to redirect their talents to peaceful civilian research, thus helping to prevent the proliferation of their expertise.

- The Biotechnical Redirection Program focuses on the redirection of former biological weapons (BW) production facilities toward peaceful uses and accelerated drug and vaccine development.

- The International Counterproliferation Program (ICP) provides training, equipment, and technical assistance and is designed to enhance detection, investigation and interdiction capabilities of border, customs, and law enforcement officials in the newly independent countries of the former Soviet Union, Eastern Europe, and the Baltic states.

- The Second-Line-of-Defense (SLD) program provides training and equipment to search, detect, and identify nuclear and other radioactive materials and deter future trafficking in illicit nuclear and nuclear-related materials.

- The Department of Justice provides technical assistance and training to prosecutors, other law enforcement officials, and criminal justice organizations focused on the development of sustainable skills and institutions that enable participating countries to more effectively combat complex and transnational crime, and build a basis upon which they can address WMD threats as well. This assistance is provided by the Department's Office of Overseas Prosecutorial Development, Assistance, and Training (OPDAT), and the International Criminal Investigative Training and Assistance Program (ICITAP).

- The Anti-Crime Training and Technical assistance (ACTTA) program helps other countries develop capacity to fight international criminal activity, drug trafficking, corruption, and trafficking in persons, which undermine public institutions, hinder development, and foster the spread of international criminal and terrorist networks.

- The Anti-Terrorism Assistance (ATA) program provides training and equipment to deter and counter the threats of terrorism. Training includes major case management, terrorist crime scene management, advanced kidnapping investigations, and financial underpinnings of terrorism.

- The Container Security Initiative (CSI) (addressed more fully in discussing U.S. efforts related to para 3 of the resolution), is designed to safeguard global maritime trade by enhancing cooperation at seaports worldwide to identify and examine high-risk containers and ensure their in-transit integrity.

- In 2002, the Department of Commerce launched the Transshipment Country Export Control Initiative (TECI) to increase cooperation and dialogue on export controls and transshipment trade with government and industry in nine major transshipment hubs: Cyprus, Hong Kong, Malaysia, Malta, Panama, Singapore, Taiwan, Thailand, and the United Arab Emirates (UAE). Under the TECI initiative the Commerce Department provides assistance to countries to encourage adoption and further development of export control systems and undertakes data exchanges to facilitate more effective administration of transshipment controls. The Department of Commerce also encourages host government development of effective controls to facilitate enforcement. The Department of Commerce also works with industry to enlist support at transshipment hubs against illicit transshipments.

***8. Calls upon all States:***

***8(a). To promote the universal adoption and full implementation, and, where necessary, strengthening of multilateral treaties to which they are parties, whose aim is to prevent the proliferation of nuclear, biological or chemical weapons;***

*Nonproliferation and Arms Control Treaties*

- Chemical Weapons Convention (CWC): The United States is a party to the Chemical Weapons Convention (CWC), which entered into force on April 29, 1997. The CWC aims to achieve a global ban on the development, production, stockpiling, transfer and use of chemical weapons. The United States strongly supports universal adherence to and full implementation of the Chemical Weapons Convention (CWC). The United States was instrumental in the development of the CWC National Implementation and Universality Action Plans that were approved and adopted by the Organization for the Prohibition of Chemical Weapons' (OPCW) top policy-making bodies and are currently being implemented by member states. The United States has strong outreach programs on universality and national implementation and provides information and assistance to States on joining and implementing the Convention. In 2004 the United States approached ninety-eight States Parties to urge adoption of measures to implement fully the Convention. The United States also urged seventeen of the thirty States not Party to join the Convention. The United States strongly encouraged Libya to join the CWC, which it has now done.

- The United States also continues to support the OPCW Technical Secretariat's (TS) efforts to promote CWC universality and national implementation. During 2003 and the first half of 2004, U.S. representatives attended OPCW–sponsored regional workshops in Sudan, Singapore, Bolivia, Senegal, Ethiopia, Malta, Romania, Uzbekistan, The Czech Republic, and Mexico on national implementation and universality. A U.S. representative will attend National Implementation Workshops projected for the remainder of 2004 in China and Kazakhstan. The United States has participated in trilateral assistance visits with Guatemala, El Salvador, Nicaragua, Slovenia and Moldova, and Poland. In late 2004, projected trilateral assistance visits are planned to Rwanda and Burundi.

- Biological Weapons Convention (BWC): The United States is party to the 1975 Biological Weapons Convention (BWC), which establishes a ban on biological and toxin weapons. Specifically, the BWC prohibits the development, production, stockpiling, acquisition and/or retention of biological or microbial agents or toxins of type and in quantities that have no justification for prophylactic, protective or other peaceful purposes; and weapons, equipment or means of delivery designed to use such agents or toxins for hostile purposes or in armed conflict. The United States has a strong outreach program to encourage other nations to join and fully implement the Convention. The United States provides information and assistance to other States on adherence to, and implementation of, the BWC.

- Treaty on the Non-Proliferation of Nuclear Weapons (NPT): The United States actively and strongly promotes universal adoption, full implementation, and strengthening of the NPT. The United States continues to urge states that have not acceded to the NPT to do so as non-nuclear weapon states (NNWS) and to place all their nuclear facilities under safeguards. The United States abides by all of its NPT obligations and participates actively in the NPT review process. The United States also participates in and provides strong support to those institutions with responsibilities related to the Treaty, including the International Atomic Energy Agency and the United Nations. At the third session of the Preparatory Committee for the 2005 Review Conference of the Parties to the NPT, the United States tabled a number of recommendations for strengthening the NPT. These included a call for universality of the Additional Protocol; adoption of the Additional Protocol as a condition of new, nuclear supply by the end of 2005; and fulfilling the obligations of UNSCR 1540.

- Convention on the Physical Protection of Nuclear Materials: The Convention on the Physical Protection of Nuclear Materials (CPPNM) establishes a legal obligation on States Parties to apply physical protection to nuclear materials used for peaceful purposes in international transport. The United States is a party to the CPPNM and has always strongly supported its goal of assuring that nuclear material used for peaceful purposes is accorded effective physical protection. In 1998, the United States launched an effort to strengthen the Convention by broadening its coverage to all nuclear material used for peaceful purposes in domestic use, storage, and transport (not just that in international transport) and by criminalizing the act of sabotage on a nuclear facility. The IAEA has circulated to all States Parties, in accordance with Article 20 of the Convention, draft proposed amendments to the CPPNM, as submitted by Austria with the support of twenty-four other

governments (including the United States). If a majority of the States Parties so request, the IAEA would convene a diplomatic conference, possibly to be held in early 2005, to consider the proposed amendments.

*Twelve Conventions and Protocols Related to Terrorism*

- The United States is a party to the twelve conventions and protocols relating to terrorism and appropriate legislation has been enacted to fully implement them.

- This includes the International Convention for the Suppression of the financing of Terrorism, which: (1) requires parties to take steps to prevent and counteract the financing of terrorists, whether direct or indirect (e.g., through groups claiming to have charitable, social or cultural goals or which also engage in such illicit activities as drug trafficking or gun running); (2) commits states to hold those who finance terrorism criminally, civilly or administratively liable for such acts; and (3) provides for the identification, freezing and seizure of funds allocated for terrorist activities, and encourages parties to consider concluding agreements for the sharing of the forfeited funds with other states on a regular or case-by-case basis. The Convention states that bank secrecy will no longer be justification for refusing to cooperate.

- The United States monitors compliance by Parties to multilateral treaties and submits an annual report, pursuant to section 403 of the Arms Control and Disarmament Act, as amended, which requires, as part of the Department of State Annual Report, a discussion of adherence to and compliance with arms control agreements and nonproliferation agreements and commitments. This report addresses U.S. compliance, and compliance by other countries that are parties to multilateral agreements, including agreements with the United States. Pursuant to Section 403(a)(6), this report, to the maximum extent practicable, identifies each and every question that exists with respect to compliance by other countries with their arms control, nonproliferation, and disarmament agreements with the United States.

***8(b). To adopt national rules and regulations, where it has not yet been done, to ensure compliance with their commitments under the key multilateral non-proliferation treaties;***

*Legislation*

- For information on U.S. efforts to adopt national rules and regulations to ensure compliance with commitments under key multilateral nonproliferation treaties, see Section 2 of this report.

***8(c) To renew and fulfil their commitment to multilateral cooperation, in particular within the framework of the International Atomic Energy Agency, the Organization for the Prohibition of Chemical Weapons and the Biological and Toxin Weapons Convention, as important means of pursuing and achieving their common objectives in the area of non-proliferation and of promoting international cooperation for peaceful purposes;***

*Organization for the Prohibition of Chemical Weapons (OPCW)*

- The Organization for the Prohibition of Chemical Weapons (OPCW) is the international organization established in 1997 by the Chemical Weapons Convention (CWC) to ensure the CWC works effectively and achieves its purpose. The United States is a permanent member of the Executive Council, one of the top-policy making organs of the OPCW, and maintains a permanent Delegation to the OPCW in The Hague. The United States actively supports the efforts of the OPCW Technical Secretariat. The United States is an active participant in the meetings of the Executive Council and annual Conference of States Parties.

*The Biological and Toxin Weapons Convention (BWC)*

- As a State Party to the Biological Weapons Convention (BWC), the United States fully supports and is actively involved in the 2003-2005 agreed Work Program of BWC States Parties. The BWC Work Program is bringing experts together to review and promote national actions on critical issues such as national implementation measures, disease surveillance, response, and mitigation, investigation of suspicious outbreaks, or alleged use, pathogen security and codes of conduct for scientists. The United States attends and actively participates in the annual Experts Meetings and meetings of BWC States Parties.

*International Atomic Energy Agency*

- The United States successfully led international efforts to increase the IAEA's regular budget for safeguards. In addition, the United States has provided over $50 million in voluntary cash and in kind assistance to the IAEA in each of the last four years.

- The United States is also calling for a special committee of the IAEA Board of Governors to focus intensively on safeguards and verification and strengthen the IAEA's ability to ensure compliance with international non-proliferation obligations.

- The United States continues to encourage IAEA Board members to adopt the policy that states under investigation because of significant safeguards failings should not be selected to serve on the Board or the Special Committee and should not participate in decisions by either body regarding their own cases.

- The United States strongly supported and continues to support establishment and implementation of common international guidelines governing exports and imports of high-risk radioactive materials to prevent their diversion and use in radiological dispersion devices. The IAEA approved and issued a major revision to the Code of Conduct on the Safety and Security of Radioactive Sources (Code of Conduct), which can be found at http://www.iaea.org/Publications/Standards/index.html. The United States also played a key role in multilateral efforts to develop a corresponding guidance document for export and import

activities involving high-risk radioactive material. This guidance document will likely be approved for publication as an IAEA Information Circular (INFCIRC) in the near future.

*Updating Australia Group Control Lists*

- The United States has proposed and the Australia Group adopted the addition of eight new toxins to the Australia Group Control List as well as new controls on related equipment to make the development of WMD more difficult for both state and non-state proliferators. The United States has also championed the addition of "catch-all" controls within the Australia Group and other export control regimes to limit the ability of all proliferators to easily gain access to any commodity, controlled or not, or any relevant service or contract and thus deny aid to proliferators in any way, shape or form.

***8 (d) To develop appropriate ways to work with and inform industry and the public regarding their obligations under such laws;***

*Nuclear Industry Outreach*

- Senior officials of the Office of Export Control Policy and Cooperation (NA-242), Department of Energy/National Nuclear Security Administration (DOE/NNSA), participate regularly in meetings with industry on compliance with U.S. Government export control laws and regulations, and with non-governmental organizations (NGO) concerned with nuclear nonproliferation issues. NA-242 presentations focus on DOE regulations relating to "Assistance to Foreign Atomic Energy Activities." See 10 C.F.R. § 810. These programs detail recent statutory and regulatory developments, discuss issues raised by industry and NGOs, and encourage direct dialogue on cases that may raise proliferation concerns.

- In addition to direct contacts with industry and NGOs, DOE/NNSA export control specialists maintain close contacts with the DOE national laboratories and other facilities, who in turn work with contactors and pass on DOE/NNSA export control guidance. Further, in the near future, export control personnel throughout the DOE/NNSA complex will have access to the NA-242 Website, which offers current export control regulations and guidance on sensitive technologies and countries, as well as pertinent news developments. These personnel will be better able to advise contractors on export control and proliferation concerns.

- To enhance communications with internal and external stakeholders on emergency preparedness policies, regulations and programs for currently licensed and potential new power reactors, NRC integrated emergency preparedness and incident response functions into the Office of Nuclear Security and Incident Response and increased the resources devoted to such communications.

- NRC engaged in extensive deliberations with interested and authorized stakeholders to communicate proposed plans and obtain feedback in the development of more than 30 security

Orders issued since September 11, 2001. They have also been involved in the ongoing comprehensive security review and vulnerability assessments as appropriate.

- NRC established a protected server system specifically designed to make it possible to communicate sensitive information (such as security alert advisories) with authorized licensee personnel and authorized State officials.

- NRC and DHS co-sponsored a two-day Integrated Response Homeland Security Workshop at NRC headquarters to exchange information with approximately 300 participants including State Liaison Officers, State Radiation Control Directors, and other Federal and State government organizations. The NRC public web site http://www.nrc.gov/ has been significantly updated to provide meaningful information to the public in a manner that balances public access with protection of sensitive security information.

- In August 2003, NRC established the position of Director of Communications to provide integrated leadership and direction for NRC external communications and to enhance the effectiveness of NRC's communications with the public, the media, and the Congress in support of NRC's strategic goals.

*Financial Services, Charities*

- The Department of Treasury works closely with the private sector, the non-profit sector and the public at large to inform them of their obligations under law. Non-profit charities are often targeted as financial channels exploited and used by terrorists and their supporters. In response to this threat, in November of 2002, the U.S. Treasury Department released Anti-Terrorist Financing Guidelines: Voluntary Best Practices for U.S.-Based Charities to enhance donor awareness of the kinds of practices that charities may adopt to reduce the risk of terrorist financing. These Guidelines are voluntary and do not supersede or modify legal requirements applicable to non-profit institutions. Rather, they are intended to assist charities in developing a risk-based approach to guard against the threat of terrorist abuse. Charities and donors are encouraged to consult these Guidelines in considering their own protective measures that will allow them to continue serving important and legitimate interests while simultaneously preventing surreptitious infiltration or abuse by terrorist groups.

- The Department of Treasury releases information publicly which may help ensure that certain assets are blocked and transactions via U.S. persons are terminated. Treasury is also the hub for dissemination of information and guidance on U.S. sanctions programs. Equally important is Treasury's monitoring role and its coordination with federal regulatory agencies to provide for continuous information sharing.

- The Department of Treasury's OFAC provides a unique service through its toll-free telephone Hotline, giving real-time guidance on in-process transactions. The hotline averages 1,000 calls every week with at least $1 million, and sometimes as much as $35 million, in appropriately

interdicted items each week. The Hotline allows OFAC to stop illicit transactions before they are processed. In addition, in July 2003, Treasury created an e-Hotline that allows U.S. persons with in-process transactions to send an e-mail to OFAC containing the specifics of the transaction in question. OFAC has received more than 600 inquiries via the e-Hotline. Treasury's ability to stop in-process transactions before they are processed has become a benchmark, especially in the war on terrorist financing.

- The Department of Treasury's OFAC website contains over 1,000 documents, receives over a million hits per month, and has attracted 15,000 email subscribers—so that all affected parties can receive notification anytime OFAC makes a new designation or a change to one of its sanctions programs.

- The Department of Treasury's outreach expands beyond banks to include the securities industry, exporters and importers, insurance companies, title companies, and car dealerships. The availability of "interdiction" software from private vendors has significantly increased industry's ability to facilitate interdictions. This software has promoted the creation of a very effective "web" within the United States through which a target transaction is unlikely to escape.

- The Department of Treasury's FinCEN works closely with the financial services industries to ensure that the regulations it crafts strike the appropriate balance between meeting the needs of the government, the regulatory burden imposed upon the financial industry, and the privacy interests of U.S. citizens. FinCEN's approach to assuring industry compliance with the Bank Secrecy Act is predicated on education and outreach. FinCEN employs a variety of techniques and media outreach, including a public web site, http://www.fincen.gov/.

- Pursuant to Section 314(a) of the USA PATRIOT Act, FinCEN now assists U.S. law enforcement investigations involving terrorism or significant money laundering by transmitting to thousands of financial institutions information from law enforcement about individuals and entities about whom there is credible evidence of terrorism or significant money laundering activity.

- FinCEN's use of Financial Advisories and notifications to financial institutions on systemic financial crime trends, such as the criminal use of foreign bank drafts, continues to be important in communicating financial crime concerns to the private financial sector. These Financial Advisories are flexible, and may be tailored immediately to meet new and evolving threats for terrorist financing and financial crimes. FinCEN also has a 24-hour "Hotline" by which financial institutions submit suspicious activity reports (SAR's) associated with terrorist financing for rapid distribution to law enforcement. Hundreds of "Hotline" SARS are received and forwarded to appropriate agencies for their information or action as required.

- Additionally, the IRS conducts outreach efforts through each of its 35 field offices, through 41 Suspicious Activity Report Review Teams (SAR-RT) and through 7 High Intensity Financial Crime Area (HIFCA) designations. These outreach efforts include BSA basic training regarding Suspicious Activity Reports and refresher training for bank and non-bank financial institutions as

well as law enforcement. The IRS has also conducted financial investigative training/seminars for analysts from U.S. intelligence agencies.

*Department of Commerce Outreach to Dual-Use Exporters*

- The Department of Commerce conducts outreach with U.S. industry and others who must comply with U.S. export controls and multilateral regime commitments through a variety of activities. These activities range from large seminars, to industry seminars on topics of special interest, to soliciting industry views through technical advisory committees, to one-on-one counseling for exporters.

- The Department of Commerce works closely with industry through meetings, conferences, and seminars to make industry aware of their export control obligations. Commerce has a comprehensive seminar program. These programs provide guidance to new and established exporters regarding the EAR and changes in export policy and licensing procedures. Seminars range from a one-day seminar program that covers the major elements of the U.S. dual-use export control system to a two-day program that provides a more comprehensive presentation of exporter obligations under the EAR. Commerce also conducts workshops on topics of specialized interest, such as technology controls, including encryption and deemed exports, freight forwarder compliance, and implementation of export management systems.

- With respect to industry's role and U.S. commitments in the multilateral export control regime context, the Department of Commerce also actively conducts outreach to U.S. industry affected by multilateral regimes (e.g., Australia Group, OPCW and IAEA). In preparation for ratification of the Additional Protocol, the Department of Commerce hosted an outreach seminar for representatives from the Nuclear Energy Institute (NEI) regarding its role in implementing the Additional Protocol, and continues to consult with NEI on the impact of the Additional Protocol on U.S. industry. The Department of Commerce also participates in conferences for the commercial nuclear industry, informing participants of Commerce's prospective role in implementation of the Additional Protocol.

- In addition, the Department of Commerce's Bureau of Industry and Security holds an annual Update Conference on Export Controls and Policy. The conference, which has been held for the last 16 years, is Commerce's premier export control outreach event. The Update Conference provides information on U.S. export control policies, regulations, and procedures to a cross-section of U.S. industry representatives and export control practitioners. A variety of U.S. government officials including representatives from the Departments of Commerce, State, Defense and other agencies participate in this event and interact with industry representatives.

- The Department of Commerce enforcement authorities also conduct outreach: to train U.S. exporters to identify and avoid illegal transactions; to reduce U.S. business participation in foreign boycotts through a comprehensive public awareness program; to improve government-wide export enforcement efforts through increased cooperation with other U.S. Government export control and

enforcement agencies; and to establish working relationships with foreign export enforcement authorities. Through Project Outreach, special agents visit approximately 1,100 exporting firms annually to help the business community prevent export violations. Department of Commerce enforcement authorities also conduct seminars at the Department of Energy nuclear laboratories to educate senior officials and scientists about export control requirements

- The Department of Commerce also supports efforts by public and private sector organizations to introduce the Department of Commerce's Bureau of Industry and Security's mission and services to audiences in specific business and technology sectors by providing speakers for continuing education programs. Participation in these events provides Department of Commerce officials with greater insight into technology and market developments in key sectors of the economy. In addition to educating U.S. companies, Department of Commerce also conducts international export control outreach seminars to provide key export control-related information to companies outside the United States that use or re-export: (1) U.S.-origin parts and components for manufacturing and assembly and/or (2) U.S. origin systems, software, or technology to develop foreign-made products.

- In an effort to solicit views from industry on technology and the development of export control regulations, the Department of Commerce has established technical advisory committees to provide a forum for discussion of these issues. There are six Technical Advisory Committees (TACs) covering information systems, materials, materials processing equipment, regulations and procedures, sensors and instrumentation, and transportation and related equipment. The TACs advise the Department of Commerce on export control issues, including proposed revisions to multilateral export control lists, licensing procedures that affect export controls, and assessments of foreign availability of controlled products. TAC industry representatives are selected from firms producing a broad range of goods, technologies, and software.

- In addition, the President's Export Council Subcommittee on Export Administration (PECSEA) provides advice on U.S. policies of encouraging trade with all countries with which the United States has diplomatic or trading relations and of controlling trade for national security, foreign policy, and short supply reasons. Members are drawn from the President's Export Council, high-level federal Government officials, and representatives of business and industry who are exporters of those goods and technical data that are presently under control.

- Department of Commerce regulatory specialists assist people in one-on-one counseling sessions through phone calls, visits, and e-mails to Commerce's Outreach and Educational Services Division in Washington, D.C., and Commerce's Bureau of Industry and Security's Western Regional Office in California. These sessions provide guidance on regulations, policies, and practices that affect the particular company's export operations, and help increase compliance with U.S. export control regulations. Department of Commerce has implemented an e-mail notification program through its Web site, www.bis.doc.gov, whereby exporters may subscribe to receive information about BIS seminars and training programs. In addition, exporters may now sign up to

receive e-mail notification of Web site changes, regulations, press releases, and other information relating to the administration of export controls.

- Department of Energy officials also participate regularly in meetings with industry on compliance with U.S. Government export control laws and regulations, and with non-governmental organizations concerned with nuclear nonproliferation issues. DOE inputs generally focus on DOE regulations 10 CFR Part 810 regarding "Assistance to Foreign Atomic Energy Activities." DOE officials detail recent statutory and regulatory developments, discuss issues raised by industry and NGOs, and encourage direct dialogue on cases that may raise proliferation concerns.

***9. Calls upon all states to promote dialogue and cooperation on nonproliferation so as to address the threat posed by proliferation of nuclear, chemical, or biological weapons, and their means of delivery.***

- Preventing the proliferation of weapons of mass destruction and their means of delivery is a top foreign policy priority for the United States. The United States believes that more dialogue -- bilaterally, regionally, multilaterally, and internationally -- is needed to establish the WMD proliferation threat as real and serious and as one that affects all nations' security. To this end, the United States has worked to ensure that nonproliferation is a topic of discussion in various fora, including: the United Nations; the IAEA; the CWC, BWC, and NPT; the Conference on Disarmament; multilateral export control regime discussions; the ASEAN Regional Forum (ARF) and its related dialogues; APEC; the Egmont Group of Financial Intelligence Units; the Organization of American States (OAS); the Special Conference on Security in the Americas; and the Defense Ministerial of the Americas.

- In its bilateral relations, the United States places a premium on discussing and addressing the threat of WMD. The United States seeks to promote greater awareness of and cooperation on efforts needed to prevent the proliferation of nuclear, chemical, biological weapons and their means or delivery. Paragraph 7 of this report details the extensive cooperation and assistance that the United States is providing to other countries to facilitate their capabilities to detect and prevent WMD proliferation.

***10. Further to counter that threat, calls upon all States, in accordance with their national legal authorities and legislation and consistent with international laws, to take cooperative action to prevent illicit trafficking in nuclear, chemical or biological weapons, their means of delivery, and related materials;***

- U.S. efforts to take cooperative action to prevent the illicit trafficking in nuclear, chemical, or biological weapons, their means of delivery, and related materials are embodied in the Proliferation Security Initiative (PSI). President Bush announced the PSI on May 31, 2003. The PSI is a counterproliferation effort aimed at interdiction of shipments of weapons of mass destruction, their delivery systems, and related materials flowing to or from states or non-State actors of proliferation concern. On September 4, 2003, PSI partners agreed and published the PSI

"Statement of Interdiction Principles" (SOP), which identifies steps necessary for effective interdiction efforts. Since the PSI was announced, the United States has cooperated with other countries to prevent illicit trafficking in nuclear, chemical, and biological weapons, their delivery systems, and related materials at sea, in the air, or on land. These efforts have resulted in a number of successful interdictions, including of the "BBC China," a ship that was carrying a large quantity of gas centrifuge equipment to Libya.

- The United States has encouraged other states to endorse the SOP and to establish concrete readiness to assist in interdiction activities. Working with many other nations, the United States has developed and is implementing a series of training exercises through which states are enhancing their operational capabilities, raising their awareness of steps that are necessary for successful interdiction, and establishing better communications and closer relationships for effective interdiction partnerships.

- The United States has proposed negotiation of bilateral maritime boarding agreements with key flag states in support of PSI, that will facilitate consent to board vessels suspected of carrying cargo of proliferation concern. To date, three such agreements have been negotiated and signed with Liberia, Panama, and the Marshall Islands.

- On February 11, 2004, President Bush called for the work of PSI to expand to include shutting down proliferation networks. The President called on PSI participants to enhance cooperation in law enforcement, intelligence, and military channels to identify where proliferation facilitators are operating, shut them down, and bring them to full justice. The United States is working to develop guidelines to assist in the expanded work of PSI and is continuing to advance PSI's goal of establishing a global web of counterproliferation partnerships.

[1] Furthermore, under the Arms Export Control Act (AECA) – *see infra* – the unlicensed export of the delivery systems for nuclear weapons, as well as technical data and defense services relating to such systems, would be a violation because such systems and related technical data/services are included within Category IV of the International Trafficking in Arms Regulations (ITAR) as "launch vehicles, guided missiles, ballistic missiles, rockets, torpedoes, bombs." (22 C.F.R. 121.1) Also, under the Missile Technology Control Regime Annex, some items – e.g., ballistic missile systems, UAVs and rocket stages – are controlled by both the Department of Commerce on the Commerce Control List and the Department of State as U.S. Munitions List items.

[2] Pub. L. No. 83-703

[3] Pub. L. No. 93-438

[4] 42 U.S.C. § 2201

[5] 42 U.S.C. § 2201

[6] 42 U.S.C. § 2236

[7] 42 U.S.C. § 2271

[8] 42 U.S.C. § 2273

[9] 42 U.S.C. §§ 2274, 2275, 2276, 2277

[10] 42 U.S.C. § 2283

[11] 42 U.S.C. § 2284

[12] 42 U.S.C. § 2073

[13] Special nuclear material of low strategic significance, special nuclear material of moderate strategic significance, formula quantities of strategic special nuclear materials and source material at enrichment plants.

[14] 42 U.S.C 2201

[15] For example, a money service business filed a Suspicious Activity Report concerning a customer who was selling – via the Internet - chemicals potentially associated with nuclear weapons. Another example involved substantial and unusual international financial activity involving a former foreign government official associated with nuclear programs.

[16] See 31 U.S.C. 5318(g)(3).

[17] In addition to SARs and CMIRs, domestic financial institutions and certain other entities are required to file currency transaction reports (CTRs, or Form 8300s in the case of non-financial trades or businesses) for cash transactions exceeding $10,000, foreign bank account reports (FBARs) for foreign financial accounts exceeding $10,000, and forms registering as money services businesses.

[18] 18 U.S.C. § 2339A

[19] 18 U.S.C. § 2339A

[20] 18.U.S.C. § 2339B

[21] 12 U.S.C. § 2339B

[22] 8 U.S.C. § 1189

[23] 18 U.S.C. § 981 (a)(1)(A) would authorize forfeiture for the transaction offense, and 18 U.S.C. § 981 (a) (1)(C) would authorize forfeiture for the proceeds offense.

[24] The Export Administration Act (EAA) is currently maintained in force under the authority of the International Emergency Economic Powers Act (IEEPA).

[25] Note that other AEA prohibitions can include penalties of up to life imprisonment for the unauthorized disclosure or tampering with restricted data related to nuclear weaponry.

[26] Pub. L. No. 95-242

[27] 8 U.S.C. § 1189